IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL INTERNO EN LA GERENCIA DE PRODUCCIÓN DE HELM BANK, PARA DAR CUMPLIMIENTO A LA LEY SARBANES OXLEY (SOX)

XENIA ALCIRA PACHECO BALLESTEROS

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA ESI-26
BOGOTÁ, COLOMBIA
2015

IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL INTERNO EN LA GERENCIA DE PRODUCCIÓN DE HELM BANK, PARA DAR CUMPLIMIENTO A LA LEY SARBANES OXLEY (SOX)

XENIA ALCIRA PACHECO BALLESTEROS

TRABAJO DE GRADO (para optar por el título de Especialista en Seguridad Informática)

CÉSAR IVÁN RODRÍGUEZ SÁNCHEZ-MIEEE, CISSP (Tutor Temático Trabajo de Grado)

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA ESI-26
BOGOTÁ, COLOMBIA
2015

Nota de Aceptación:

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 13 de Noviembre de 2015

Dedicado a Dios, a mis Padres y a mi Familia

AGRADECIMIENTOS

Especialmente a mis Padres por animarme y apoyarme a crecer profesionalmente.

Al Equipo de Trabajo de Banco Corpbanca por permitirme participar en éste proyecto y adquirir experiencia profesional, entre ellos quiero agradecer a Néstor Fernando Vanegas Moreno - Jefe Gerencia de Riesgo Operativo y Seguridad, Jhon Jaider Morales Cano - Analista SOX Gerencia de Riesgo Operativo y Seguridad, José Luis Merchán Ortega - Gerente de Producción y Diana Paola Granados Castaño - Asesor Gerencia de Procesos.

Al Ingeniero César Iván Rodríguez Sánchez por su asesoría como Tutor temático.

Y a todas aquellas personas que hicieron posible que éste proyecto saliera adelante.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

GLOSARIO

ADR´s: American Depository Receipts - Certificado de Depósito Americano. Tomado de diapositivas Presentación Final Gerentes.pptx y Escuela Virtual Corpbanca, Cursos Normativos 2015, Módulo SARO, PCN 2015 y Seguridad de la Información (PCN2015).

AMV: Auto-regulador del Mercado de Valores. Tomado del SP1309 Subproceso Incidencias y Planes de Acción del Modelo de Control Interno SOX.

AUDITORÍA AUTO-EVALUACIÓN: Pruebas de efectividad que realizan los propios responsables del control ó personal de la misma área. Tomado del Formato de Certificación FT1552 Prueba Controles MCI-SOX.xls y diapositivas Guía de Certificación de Controles MCI-SOX Dic 2014.pdf.

AUDITORÍA PRUEBAS CRUZADAS: Pruebas realizadas por personal diferente al responsable del control y sin ningún tipo de relación jerárquica con éste (Personas de otra área). Tomado del Formato de Certificación FT1552 Prueba Controles MCI-SOX.xls y diapositivas Guía de Certificación de Controles MCI-SOX Dic 2014.pdf.

COSO: Committee of Sponsoring Organizations of the Treadway Commission. Tomado de diapositivas COSO actualización tecnología.pptx y diapositivas Presentación Final Gerentes.pptx.

ENTES DE CONTROL EXTERNO: Hace referencia a la Superintendencia Financiera de Colombia, Revisoría Fiscal, Auto-regulador del Mercado de Valores (AMV), Contralor Normativo, entre los principales. Tomado del SP1309 Subproceso Incidencias y Planes de Acción del Modelo de Control Interno SOX.

ENTES DE CONTROL INTERNO: Se refiere a la Contraloría Interna. Tomado del SP1309 Subproceso Incidencias y Planes de Acción del Modelo de Control Interno SOX.

EVIDENCIAS DE LA PRUEBA: Se deben anexar todas las evidencias de la prueba efectuada. Puede utilizarse para anexar las evidencias según el tamaño de la muestra analizada. Se debe indicar si la evidencia es automática ó documental e incluir la descripción correspondiente. Tomado del Formato de Certificación FT1552 Prueba Controles MCI-SOX.xls.

HERRAMIENTA DE GESTIÓN DOCUMENTAL: Aplicativo “DocManager”, administrado por el Área de Procesos. Tomado del SP1313 Subproceso Gestión Proceso de Certificación Modelo de Control Interno SOX.

INCIDENCIA: Se refiere a debilidades de control y deficiencias significativas. Tomado del SP1309 Subproceso Incidencias y Planes de Acción del Modelo de Control Interno SOX.

MCI: Modelo de Control Interno. Tomado del SP1313 Subproceso Gestión Proceso de Certificación Modelo de Control Interno SOX.

MODELO DE CONTROL INTERNO: En cumplimiento de la "Circular Externa 038" de 2009 emitida por la Superintendencia Financiera de Colombia, el "Modelo Corporativo de Control Interno" se implementó como la metodología corporativa Sarbanes-Oxley (SOX). Mediante este esquema se definen los procesos transversales, desarrollados de principio a fin por cada tema o producto, realizando la identificación y definición simultánea de los riesgos y controles. Tomado del MG1012 Manual General Gestión de Procesos Modelo de Control Interno.

RIESGO OPERATIVO: Posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Ésta definición incluye el riesgo legal y reputacional, asociados a tales factores. Tomado del SP1310 Subproceso Valoración del Riesgo Operativo.

SCI: Sistema de Control Interno. Tomado de Escuela Virtual Corpbanca, Cursos Normativos 2015, Módulo SARO, PCN 2015 y Seguridad de la Información (PCN2015).

SEC: Security Exchange Comision. Tomado de Escuela Virtual Corpbanca, Cursos Normativos 2015, Módulo SARO, PCN 2015 y Seguridad de la Información (PCN2015).

SOX: Sarbanes-Oxley. Tomado del SP1309 Subproceso Incidencias y Planes de Acción del Modelo de Control Interno SOX y del SP1313 Subproceso Gestión Proceso de Certificación Modelo de Control Interno SOX.

Las definiciones mencionadas en éste glosario fueron tomadas de la documentación de Banco Corpbanca Colombia, mencionada a continuación:

- ✓ Intranet Corporativa, Herramienta DocManager, Sección Manuales, Bogotá, Octubre 2015

- ✓ Escuela Virtual Corpbanca, Cursos Normativos 2015, Módulo SARO, PCN 2015 y Seguridad de la Información (PCN2015),Bogotá, Agosto 2015

- ✓ SP1309 Subproceso Incidencias y Planes de Acción del Modelo de Control Interno SOX, Última fecha publicación 15 de Septiembre de 2015, Versión 7, Código SP1309, Publicado en Herramienta de Gestión Documental - Aplicativo "DocManager"

- ✓ SP1310 Subproceso Valoración del Riesgo Operativo, Última fecha publicación 22 de Diciembre de 2015, Versión 5, Código SP1310, Publicado en Herramienta de Gestión Documental - Aplicativo "DocManager"

- ✓ SP1313 Subproceso Gestión Proceso de Certificación Modelo de Control Interno SOX, Última fecha publicación 15 de Septiembre de 2015, Versión 9, Código SP1313, Publicado en Herramienta de Gestión Documental - Aplicativo "DocManager"

- ✓ MG1012 Manual General Gestión de Procesos Modelo de Control Interno, Última fecha publicación 27 de Junio de 2015, Versión 4, Código MG1012, Publicado en Herramienta de Gestión Documental - Aplicativo "DocManager"

- ✓ Gerencia de Riesgo Operacional y Seguridad, Sistema de Control Interno Modelo SOX Corpbanca-Helm, [diapositivas Presentación Final Gerentes.pptx], Bogotá, Febrero de 2014

- ✓ Gerencia de Riesgo Operacional y Seguridad, Actualización COSO 2013 Vicepresidencia de Tecnología, [diapositivas COSO actualización Tecnológia.pptx], Bogotá, Agosto de 2015

- ✓ Gerencia de Riesgo Operacional y Seguridad, Guía de Certificación de Controles MCI-SOX Vicepresidencia de Riesgo, [diapositivas Guía de Certificación de Controles MCI-SOX Dic 2014.pdf], Bogotá, 18 de Febrero de 2015

- ✓ Gerencia de Riesgo Operacional y Seguridad, [Formato FT1494 Matriz de Riesgos y Controles SOX.xls], Bogotá, 01 de Octubre de 2015

- ✓ Gerencia de Riesgo Operacional y Seguridad, [Formato FT1552 Prueba Controles MCI-SOX.xls], Bogotá, 01 de Octubre de 2015

RESUMEN

Los Grupos Financieros que cotizan en la Bolsa de Valores de Nueva York deben acogerse a la Ley SOX (Sarbanes-Oxley) como Modelo de Control Interno.

Ahora que Helm Bank y sus Filiales hacen parte del Grupo Financiero Corpbanca Colombia S.A. y además cotiza en la Bolsa de Valores de Nueva York, lleva al Banco a implementar un Modelo de Control Interno que tenga cumplimiento con la Ley SOX (Sarbanes-Oxley) y a seguir dichos lineamientos los cuales permitirán mitigar los riesgos, elaborar controles internos en todas las área del Banco, y cumplir la normatividad y regulaciones que aplican a la organización, contribuyendo de ésta manera a los requerimientos por parte de los entes de control.

Bajo éste punto de vista, el alcance del desarrollo de éste proyecto está delimitado en la implementación de un Sistema de Control Interno en las 5 Direcciones que hacen parte de la Gerencia de Producción de Helm Bank, realizando un análisis detallado a los riesgos y controles que serán objeto de Certificación Sox por parte de la Gerencia y de revisión posterior por los Entes de Control.

Auditoría Interna y Externa, Certificación Sox, Controles, Entes de Control, Incidencias, Modelo de Control Interno, Riesgos, Sistema de Control Interno, Sox.

INTRODUCCIÓN

Como resultado de la compra del Banco Helm Bank por parte de Corpbanca Colombia S.A. a partir del 01 de Junio de 2014, inició una fase de fusión legal entre éstas 2 Entidades Financieras y producto de ésta integración, se trasladaron beneficios a los clientes a nivel de servicio, integridad del negocio y fortalecimiento en el portafolio de productos.

La formalización de ésta fase de fusión legal, implicó cambios internos dentro de la Organización entre los que se destaca la consolidación de estados financieros, el reporte a Entes de Control y contrapartes, modificaciones en plataformas tecnológicas y en las políticas de procesos de control interno.

En este tipo de integraciones financieras, es de vital importancia prevenir la ocurrencia de fraudes originados tanto en el interior como en el exterior de la organización que pueda afectar el buen nombre de la Entidad Financiera, por lo que se debe aumentar la integridad, confiabilidad y disponibilidad tecnológica en las operaciones y minimizar todo riesgo financiero.

Ahora que Helm Bank y sus Filiales hacen parte del Grupo Financiero Corpbanca Colombia S.A. y además de que la Casa Matriz Corpbanca Chile cotiza en la Bolsa de Valores de Nueva York, lleva al Banco a implementar un Modelo de Control Interno que tenga cumplimiento con la Ley SOX (Sarbanes-Oxley) y a seguir dichos lineamientos los cuales permitirán mitigar los riesgos, elaborar controles internos en todas las área del Banco, y cumplir la normatividad y regulaciones que aplican a la organización, contribuyendo de ésta manera a los requerimientos por parte de los entes de control.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Implementar en Helm Bank y específicamente en la Gerencia de Producción un Sistema de Control Interno para dar cumplimiento a la Ley Sarbanes-Oxley (SOX).

1.2 OBJETIVOS ESPECÍFICOS

- ✓ Realizar una gestión adecuada para detectar y evaluar los riesgos en cada una de las actividades realizadas en la Gerencia de Producción de acuerdo al Sistema de Administración de Riesgos existente.

- ✓ Definir y elaborar los controles internos de acuerdo a los Procesos, Subprocesos y Procedimientos existentes en la Entidad, para las 5 Direcciones de Tecnología que conforman la Gerencia de Producción.

- ✓ Aportar en la prevención y disminución de ocurrencia de fraudes, originados tanto al interior como al exterior de la Entidad, teniendo en cuenta los 3 principios básicos con los que cuenta la Organización: Autocontrol, Autoregulación y Autogestión.

- ✓ Contribuir en la Organización con el cumplimiento de la normatividad y regulaciones aplicables a la Organización como es la Circular Externa 038 de 2009 de la Superintendencia Financiera y la Ley SOX, realizando seguimiento a los planes de acción del año 2014, de los informes emitidos por los Entes de Control Interno (Contraloría) y Externo (Revisoría Fiscal).

- ✓ Proporcionar un grado de seguridad razonable en el Banco Unificado, en cuanto la consecución de los objetivos relacionados con las operaciones, la información y el cumplimiento de políticas y mecanismos de prevención.

2. PLANTEAMIENTO DEL PROBLEMA

2.1TÍTULO

Implementación de un Sistema de Control Interno en la Gerencia de Producción de Helm Bank, para dar cumplimiento a la Ley Sarbanes-Oxley (SOX).

2.2 FORMULACIÓN DEL PROBLEMA

¿La implementación de un Sistema de Control Interno le permitirá a Helm Bank identificar, analizar y mitigar posibles riesgos en el Área de Tecnología y diseñar los controles adecuados?

2.3 LÍMITES DE LA INVESTIGACIÓN

Para éste Trabajo de Grado, la implementación de un Sistema de Control Interno para el cumplimiento de la Ley SOX se delimita inicialmente a la Gerencia de Producción de la Vicepresidencia de Tecnología de Helm Bank, gestionando de forma adecuada los Riesgos y elaborando Controles internos de acuerdo a los procesos, subprocesos y procedimientos existentes en ésta Gerencia. La línea de investigación se centra en la Gestión de la Seguridad y el Riesgo.

2.4 JUSTIFICACIÓN

Tras esta fase de Fusión Legal, el Banco unificado continúa trabajando en el proceso de integración tecnológica y operativa y ha dispuesto un gran equipo de profesionales que se encuentran trabajando en los desarrollos necesarios para la integración de la plataforma que combina la tecnología de comunicaciones e información de ambas marcas. Una vez se complete la integración operativa, que depende en su gran mayoría de los sistemas y aplicaciones tecnológicas, entrará a funcionar bajo una sola marca.

La Ley Sarbanes-Oxley, promueve que todas las empresas que cotizan en la Bolsa de Valores de los Estados Unidos de América, aseguren la existencia y funcionamiento adecuado de Controles Internos en las diferentes regiones

geográficas donde operan, todo esto con el objetivo de garantizar la transparencia de sus operaciones.

Bajo el Artículo 404 de la Ley Sarbanes-Oxley, la Alta Gerencia debe realizar una evaluación anual de los controles internos. El reporte de los controles internos debe incluir:

- ✓ La declaración de la responsabilidad gerencial (CEO y CFO) para establecer y mantener controles internos para la elaboración de estados financieros de la compañía.

- ✓ La documentación que permita identificar el marco de referencia usado por la gerencia para evaluar la efectividad de los controles internos.

- ✓ La evaluación de la gerencia acerca de la efectividad de los controles internos, al término del último ejercicio fiscal de la compañía.

- ✓ Un documento indicando que el equipo de auditoría está conforme con la evaluación de los controles internos realizada por la Gerencia.

La Vicepresidencia de Tecnología de Helm Bank se encuentra a cargo de varias Gerencias que están encaminadas a dar cumplimiento con todo lo requerido en temas de fusión legal y con ello los procesos, procedimientos y cumplimiento de la Ley. La Gerencia de Producción hace parte de una de éstas Gerencias y en ella fue necesario realizar la implementación de un Sistema de Control Interno.

3. MARCO TEÓRICO

3.1 MARCO HISTÓRICO

3.1.1 Historia de la Ley SOX en Helm Bank. Los Grupos Financieros que cotizan en la Bolsa de Valores de Nueva York deben acogerse a la Ley SOX (Sarbanes-Oxley) como Modelo de Control Interno.

Las empresas chilenas deben cumplir con la Ley Sarbanes-Oxley si cotizan en la bolsa de Estados Unidos ó son subsidiarias de empresas (casa matriz) que cotizan en la bolsa de Estados Unidos.

Por lo tanto, Corpbanca Colombia – Helm Bank y sus filiales deben cumplir con la Ley Sarbanes-Oxley por ser emisor de ADR´s (*American Depository Receipts*) en el mercado de Estados Unidos. Corpbanca es un banco comercial con sede en Chile y con presencia en los mercados de Estados Unidos, España y Colombia.

3.1.1.1 Participación de la Gerencia de Riesgo Operacional y Seguridad de Helm Bank. La Gerencia de Riesgo Operacional y Seguridad posee un Modelo de Certificación de Controles (SOX), direccionado al reporte financiero, el cual responde a necesidades internas y externas en el ámbito del control para Corpbanca Colombia.

Dicho modelo considera la identificación de eventos de riesgo críticos que afecten tanto procesos de negocio como de soporte con sus respectivos controles claves y la actualización de los mismos de acuerdo a los cambios presentados.

El Modelo de Control “Certificación Controles SOX”, exige una adecuada estructura de Control Interno, responsabilizando a la alta dirección de su adecuado funcionamiento, lo anterior basado en la normativa de la Security Exchange Comision (SEC) para las sociedades que cotizan en EEUU – Ley Sarbanes-Oxley (SOX). Cada gerencia es responsable de la autoevaluación de sus riesgos y sus actividades de control asociadas, así como también la alta gerencia debe certificar sus controles a nivel de marco global.

La Gerencia de Riesgo Operacional y Seguridad a través del Área que se ha denominado SOX, posee mecanismos que le permiten identificar las deficiencias en el Modelo de Control Interno a través de:

- ✓ Proceso de Certificación de Controles SOX (Dos veces al año)

- ✓ Seguimiento a los planes de acción definidos por los responsables para el cierre de incidencias levantadas en la certificación.
- ✓ Informes emitidos por los Entes de Control Interno (Contraloría) y Externos (Revisoría Fiscal)

Dichas incidencias son presentadas al Comité de Auditoría, a Presidencia y/o a los auditorios que lo requieran.

3.1.1.2 Participación de la Gerencia de Producción y Seguridad Informática de Helm Bank. La Vicepresidencia de Tecnología, la Gerencia de Seguridad Informática y la Gerencia de Producción, cuenta con un análisis de riesgos informáticos, el cual incluye la definición de controles para reducir, mitigar, transferir ó evitar los riesgos, y debe contar con unos responsables y unos plazos de implementación de dichos controles.

También son encargados de implementar, mantener y monitorear los sistemas de gestión de seguridad de la información para la organización, manteniendo un nivel aceptable de riesgo informático en sus operaciones, aplicaciones, infraestructura tecnológica y procesos mediante la protección de la confidencialidad, integridad y disponibilidad de la información sensible para la Organización, con el fin de disminuir el riesgo de fraudes informáticos contra los clientes y las empresas del Grupo Corpbanca en Colombia.

A su vez, es responsable de la documentación y/o actualización de los Subprocesos, Procedimientos y demás documentos asociados a los mismos, con el apoyo y los lineamientos de la Gerencia de Procesos y es responsable de la identificación de los Riesgos y Controles, con el apoyo de la Gerencia de Riesgo Operativo.

De allí el alto compromiso por parte de la Gerencia de Producción y sus integrantes, en analizar, detectar y evaluar los riesgos internos en cada una de las actividades realizadas por la Gerencia de Producción de acuerdo al Sistema de Administración del Riesgos.

3.1.1.3 Participación de la Gerencia de Procesos Unificada. El Área de Procesos es el responsable de dar los lineamientos de la metodología y asesorar al dueño funcional del proceso en las definiciones requeridas, en el levantamiento y validación de la información, en la verificación de la secuencia lógica de los procedimientos y actividades, en las políticas, formatos y demás documentos de procesos. Así mismo, es responsable de la optimización y eficiencia de procesos alineados con las necesidades del Negocio.

Desde el inicio de la fusión legal entre Banco Corpbanca Colombia y Helm Bank, se realizaron mesas de trabajo por parte de las Gerencias de Procesos de las 2 marcas para cumplir con un plan de unificación y homologación de procesos integrados en cuanto a Procesos, Subprocesos y Procedimientos en todas las Áreas del Banco Unificado.

3.2 MARCO LEGAL

3.2.1 Definición Ley Sarbanes-Oxley. La Ley Sarbanes-Oxley, cuyo título oficial en inglés es Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (30 de julio de 2002), es una ley de Estados Unidos también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. También es llamada SOx, SarbOx o SOA.

La Ley Sarbanes-Oxley nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa de valores, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.

Esta ley, más allá del ámbito nacional, involucra a todas las empresas que cotizan en NYSE (Bolsa de Valores de Nueva York), así como a sus filiales.

3.2.1.1 Ley Sarbanes-Oxley – ¿Por qué nace?. La Ley Sarbanes-Oxley fue creada como una respuesta firme a los repetidos escándalos financieros y corporativos que afectaron a grandes empresas estadounidenses a fines del año 2001, producto de quiebras, fraudes y otros manejos administrativos no apropiados, que dañaron seriamente la credibilidad del sistema económico.

3.2.1.2 Objetivos de la Ley. A continuación se mencionan los objetivos principales de la ley Sox:

- ✓ Restaurar la confianza del público en el mercado público de valores.
- ✓ Mejorar el gobierno corporativo y promover prácticas éticas de negocios.
- ✓ Mejorar la transparencia e integridad de los estados financieros y sus revelaciones.
- ✓ Responsabilizar a la administración de la compañía sobre la información material que es presentada ante la Comisión de bolsa y valores de los Estados Unidos por parte de Casa Matriz.

3.2.1.3 Ley Sarbanes-Oxley - ¿A quién aplica?. La Ley aplica a todas las empresas norteamericanas y extranjeras que cotizan en la bolsa de valores de Nueva York. Esto incluye a:

- ✓ Casa Matriz
- ✓ Subsidiarias
- ✓ Afiliadas

3.2.1.4 Artículo (404) Ley Sarbanes-Oxley. La Sección 404 “Evaluación de la Gerencia de los Controles Internos” establece obligaciones por parte de la Gerencia de la compañía, en emitir un informe anual sobre la evaluación del control interno de cada uno de los procesos del negocio. Dentro de este informe de control interno se establece la responsabilidad del equipo directivo de tener una estructura de control interno adecuada. Anteriormente ésta exigencia no existía y ahora el equipo directivo es responsable ante posibles fraudes.

Principales lineamientos de la sección 404:

a) Una declaración de que la Gerencia de la compañía es responsable por el diseño, aplicación y mantenimiento de un control interno adecuado sobre la emisión de reportes financieros.

b) Una declaración que explique el marco de control interno adoptado por la compañía para la evaluación de la efectividad del control interno sobre la emisión de reportes financieros.

c) Una evaluación y juicio sobre el diseño y efectividad del control interno de la compañía sobre la emisión de reportes financieros.

d) Una declaración de cualquier debilidad material detectada durante la evaluación del control interno de la compañía sobre la emisión de los reportes financieros.

e) Un informe de los auditores externos de la compañía opinando con relación a la evaluación realizada por la Gerencia de la compañía sobre el control interno para la emisión de los reportes financieros.

Además, esta sección requiere que los auditores externos de las compañías certifiquen la evaluación del control interno realizado por la Gerencia sobre la emisión de los reportes financieros. Es decir, las organizaciones no solo deben asegurar el adecuado funcionamiento del control interno, incluyendo los controles de Tecnología de Información (IT), sino que también deberán proveer a sus auditores externos la documentación necesaria que respalde la evaluación y la decisión final de la alta Gerencia sobre el control interno.

3.2.2 Comportamiento de COSO. *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*. Es una iniciativa de 5 organismos para la mejora de control interno dentro de las organizaciones.

Un Control Interno se define como un proceso efectuado por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías:

- ✓ Eficacia y eficiencia de las operaciones.
- ✓ Confiabilidad de la información financiera.
- ✓ Cumplimiento de las leyes, reglamentos y normas (que sean aplicables).

3.2.2.1 Componentes. De acuerdo al marco COSO, el control interno consta de cinco componentes relacionados entre sí; éstos derivarán de la manera en que la Dirección dirija la Unidad y estarán integrados en el proceso de dirección. Los componentes serán los mismos para todas las organizaciones (públicas o privadas) y dependerá del tamaño de la misma la implantación de cada uno de ellos.

Los componentes son:

a) Ambiente de Control
b) Evaluación de Riesgos
c) Actividades de Control
d) Información y Comunicación
e) Supervisión y Monitoreo

3.2.2.2 Ambiente de Control. El ambiente o entorno de control es la base de la pirámide de Control Interno, aportando disciplina a la estructura. En el se apoyarán los componentes restantes, por lo que será fundamental para concretar los cimientos de un eficaz y eficiente sistema de Control Interno. Marca la pauta del funcionamiento de la Unidad e influye en la concientización de sus funcionarios.

Los factores a considerar dentro del Entorno de Control serán: La Integridad y los Valores Éticos, la Capacidad de los funcionarios de la Unidad, el Estilo de Dirección y Gestión, la Asignación de Autoridad y Responsabilidad, la Estructura Organizacional y, las Políticas y Prácticas de personal utilizadas.

3.2.2.3 Evaluación de Riesgos. Cada Unidad se enfrenta a diversos riesgos internos y externos que deben ser evaluados. Una condición previa a la

Evaluación de Riesgo es la identificación de los objetivos a los distintos niveles, los cuales deberán estar vinculados entre sí.

La Evaluación de Riesgos consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo deben ser gestionados. A su vez, dados los cambios permanentes del entorno, será necesario que la Unidad disponga de mecanismos para identificar y afrontar los riesgos asociados al cambio.

En la evaluación se deberá analizar que los Objetivos del Área hayan sido apropiadamente definidos, que los mismos sean consistentes con los objetivos institucionales, que fueran oportunamente comunicados, que fueran detectados y analizados adecuadamente los riesgos y, que se les haya clasificado de acuerdo a la relevancia y probabilidad de ocurrencia.

3.2.2.4 Actividades de Control. Las actividades de control son las políticas, procedimientos, técnicas, prácticas y mecanismos que permiten a la Dirección administrar (mitigar) los riesgos identificados durante el proceso de Evaluación de Riesgos y asegurar que se llevan a cabo los lineamientos establecidos por ella.

Las Actividades de Control se ejecutan en todos los niveles de la Unidad y en cada una de las etapas de la gestión, partiendo de la elaboración de un Mapa de Riesgos, de acuerdo a lo señalado en el punto anterior.

En la evaluación del Sistema de Control Interno no solo debe considerarse si fueron establecidas las actividades relevantes para los riesgos identificados, sino también si las mismas son aplicadas en la realidad y si los resultados obtenidos fueron los esperados.

3.3 SISTEMA DE CONTROL INTERNO (SCI)

El Sistema de Control interno está compuesto por una Normativa, una Definición para el Banco Corpbanca y unos Principios.

3.3.1 Normativa Control Interno. Circular externa 038 de la Superintendencia Financiera de Colombia de 2009.

3.3.2 Definición. Conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por la junta directiva u órgano equivalente, la alta dirección y demás funcionarios de una organización

para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos fundamentales:

- ✓ Obtener información financiera correcta y segura
- ✓ Salvaguardar los activos
- ✓ Mejorar la eficiencia y eficacia en las operaciones.
- ✓ Prevenir y mitigar la ocurrencia de fraudes, originados tanto al interior como al exterior del Grupo.
- ✓ Realizar una gestión adecuada de los riesgos.
- ✓ Aumentar la confiabilidad y oportunidad en la información generada por la organización.
- ✓ Dar un adecuado cumplimiento de la normatividad y regulaciones aplicables a la organización.

3.3.3 Principios. Constituyen los fundamentos que garantizan la efectividad del SCI, que las entidades deben incluir, documentar y tener a disposición de la Superintendencia Financiera de Colombia:

3.3.3.1 Autocontrol. Es la capacidad de todos los funcionarios independientemente de su nivel jerárquico, para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos para mejorar sus tareas y responsabilidades.

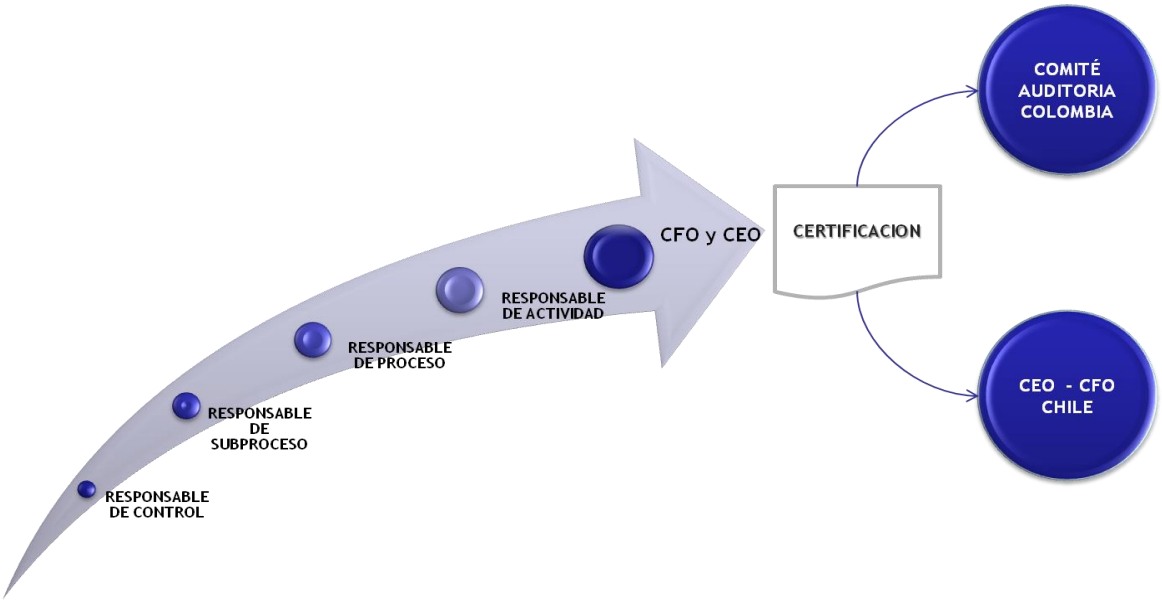
3.3.3.2 Autorregulación. Se refiere a la capacidad de la Organización para desarrollar y aplicar métodos, normas y procedimientos que permitan el desarrollo, implementación y mejoramiento del SCI.

3.3.3.3 Autogestión. Apunta a la capacidad de la Organización para interpretar, coordinar, ejecutar y evaluar de manera efectiva, eficiente y eficaz su funcionamiento.

En cumplimiento a la "Circular Externa 038" de 2009 emitida por la Superintendencia Financiera de Colombia, el "Modelo Corporativo de Control Interno" se implementa como la metodología corporativa Sarbanes-Oxley (SOX). Mediante este esquema se definen los procesos transversales, desarrollados de principio a fin por cada tema o producto, realizando la identificación y definición simultánea de los riesgos y controles, sustentado en un proceso de certificación periódica de controles (semestral) e integral (anual) bajo una estructura piramidal de responsabilidades.

En la Figura 1. Modelo Corporativo de Control Interno Corpbanca – Helm Bank de Octubre de 2014, se puede apreciar que el "Modelo Corporativo de Control Interno" exige una adecuada estructura de Control Interno, responsabilizando a la alta dirección de su adecuado funcionamiento, lo anterior basado en la normativa de la Security Exchange Comisión (SEC). Cada gerencia es responsable de la autoevaluación de sus riesgos y sus actividades de control asociadas, así como también la alta administración debe certificar sus controles a nivel de marco global.

Figura 1. Modelo Corporativo de Control Interno Corpbanca - Helm Bank Octubre 2014



Fuente Presentación Final Gerentes.pptx. Banco Corpbanca Colombia.

3.3.4 Modelo de Certificación Sox. La finalidad de ésta estructura es responsabilizar a la administración de la compañía sobre la información material que es presentada ante la comisión de bolsa y valores de los Estados Unidos por parte de Casa Matriz. El responsable de la actividad corresponde a los Gerentes encargados de las áreas y son directos responsables de que su equipo de trabajo cumpla con los Controles propuestos.

Existe el marco de control interno y el modelo de procesos específicos. El objetivo del primero es complementar la documentación incluida en el segundo, del tal forma que en ambos ámbitos queden documentados los ocho componentes del modelo de control interno (COSO - (*Committee of Sponsoring Organizations of the Tradeway Commission*)): ambiente interno de control, establecimiento de

objetivos, identificación de eventos, evaluación del riesgo, respuesta al riesgo, actividades de control, información y comunicación, y monitoreo.

En el modelo de procesos, riesgos y controles específicos, son analizados los componentes de “Evaluación del riesgo” y “Actividades de control”. Otros como “Ambiente interno de control” o “Monitoreo”, se cubren básicamente con controles generales y de supervisión, políticas generales, códigos de conducta, etc. aplicados de forma global sobre el conjunto de las sociedades, en lugar de controles específicos asignables a subprocesos.

El Sistema de Control Interno a su vez está conformado por los diferentes Sistemas de Administración de Riesgos como se observan en la Figura 2. Sistemas de Administración de Riesgos, y se definen a continuación:

SARM: Sistema de Administración de Riesgo de Mercado

SARL: Sistema de Administración de Riesgo de Liquidez

SARC: Sistema de Administración de Riesgo de Crédito

SAC: Sistema de Atención al Cliente

SARLAFT: Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo

SARO: Sistema de Administración de Riesgo Operativo

Figura 2. Sistemas de Administración de Riesgos

Fuente Cursos Normativos 2015 Escuela Virtual Corpbanca - Módulo PCN y Seguridad de la Información Agosto 2015 (PCN2015). Banco Corpbanca Colombia.

Éste último es de resaltar, ya que el objetivo de **SARO** es proporcionar un grado de seguridad razonable en cuanto la consecución de los objetivos relacionado con las operaciones, la información y el cumplimiento. Establece las políticas y mecanismos de prevención, control, evaluación y mejoramiento continuo de la entidad.

3.3.5 Componentes del Sistema de Control Interno (SCI). El Sistema de Control Interno (SCI) también tiene unos componentes relacionados a continuación:

Entorno de Control: Conjunto de normas, procesos y estructuras que constituyen la base sobre la cual desarrollar el Control Interno de la Organización.

Evaluación de Riesgos: Es un proceso dinámico e interactivo utilizado para identificar y evaluar los Riesgos. Dichos riesgos deben evaluarse en relación a unos niveles preestablecidos de tolerancia. De este modo, la evaluación de riesgos constituye la base para determinar cómo se gestionarán.

Actividades de control: Son las acciones establecidas que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos con impacto potencial en los objetivos. Las actividades de control se ejecutan en todos los niveles de la Entidad.

Información y Comunicación: La información es necesaria para que la Entidad pueda llevar a cabo sus responsabilidades de control interno y soportar el logro de sus objetivos. La comunicación interna es el medio por el cual la información se difunde a través de toda la organización que fluye en sentido ascendente, descendente y en todos los niveles de la organización.

Monitoreo: Las Evaluaciones continuas y las evaluaciones independientes o una combinación de ambas se utilizan para determinar si cada uno de los 5 componentes del Control Interno están presentes y funcionan adecuadamente.

3.3.6 Riesgo Operativo. Posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Ésta definición incluye el riesgo legal y reputacional, asociados a tales factores.

Riesgo: Es la probabilidad de que se produzca un evento y sus consecuencias negativas.

Evento: Es el Riesgo ocurrido, es la materialización (ocurrencia) de un Riesgo.

Evento de Riesgo Operativo: Materialización de un riesgo operativo que ha rebasado los controles.

Con los Riesgos se elaboran matrices de riesgo y perfiles de riesgos y con los eventos se construyen bases de eventos que luego se grafican.

3.3.7 Clasificación de los riesgos que pueden afectar a la organización. Es importante clasificar los riesgos que pueden afectar a la Organización si no logran ser controlados, como los siguientes:

Fraude Interno: Son los actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la Entidad, en los que esté implicado almenos un Empleado.

Fraude Externo: Son los actos realizados por una persona Externa a la Entidad que buscan defraudar, apropiarse indebidamente de activos de la misma Entidad ó incumplir normas ó leyes.

Relaciones Laborales: Hace referencia a los actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo, y en general, la legislación vigente sobre la materia.

Clientes: Se refiere a fallas negligentes o involuntarias en las obligaciones frente a los clientes y que impiden satisfacer una obligación profesional frente a éstos.

Daños a activos físicos: Son las pérdidas derivadas de daños y perjuicios a los activos físicos de la entidad.

Fallas tecnológicas: Son pérdidas derivadas de incidentes por fallas tecnológicas.

Ejecución y administración de procesos: Pérdidas derivadas de errores en la ejecución y administración de los procesos.

3.3.8 Identificación de los riesgos. Los Riesgos se identifican en los Procesos, por eso se documentan y se actualizan todos los procedimientos permanentemente para controlar e identificar qué se hace y quien lo hace, y de todo esto se deja evidencia para que luego la Auditoría Interna y Externa pueda realizar la respectiva validación.

Las Áreas de Procesos y de Riesgo Operacional apoyan a las áreas responsables de cada proceso en la identificación y descripción homogénea de Riesgos y Controles. Igualmente es necesario contar con unas Políticas para la administración del riesgo operativo que orientan las acciones de toda la organización. A continuación algunas de éstas políticas:

- ✓ Todo el equipo del Grupo Financiero, sin excepción, debe asegurar el cumplimiento de las normas internas y externas.

- ✓ La entidad impulsará a nivel institucional, la cultura de riesgo operacional.

- ✓ Todos los colaboradores del grupo financiero actuarán siempre teniendo en cuenta que sus intereses particulares no primen sobre los de la entidad o sus clientes, además, atenderán las normas del Código de Conducta.

- ✓ Toda persona que preste servicio en el grupo financiero deberá informar los riesgos operativos (potenciales y ocurridos) que se presenten y afecten o no (positiva ó negativamente) la cuenta de resultados.

3.3.9 Enfoque del SCI. El Sistema de Control Interno - Sox enfoca su aplicación en 2 ámbitos: El Modelo de Marco Global y el Modelo de Procesos Específicos.

El modelo de Marco Global: Hace referencia a los aspectos que afectan estructuralmente a toda la organización, por ejemplo, poseer un código de conducta y realizar una adecuada selección de personal.

El Modelo de Procesos Específicos: Son aquellas actividades que se desarrollan y afectan puntualmente un proceso, por ejemplo, Un préstamo con garantía personal, contratación, administración y seguimiento de productos y Leasing.

Con el fin de asegurar que estos modelos sean implementados por el equipo de trabajo, anualmente se desarrollan 2 actividades de evaluación, donde los Gerentes de las diferentes áreas son los encargados de certificar la correcta implementación y ejecución de los controles del Modelo de Procesos Específicos.

Éste ejercicio se hace de igual manera para el Modelo de Marco Global donde son los Vicepresidentes los encargados de la certificación. Finalmente la Presidencia y Vicepresidencia recogen éstos informes y emiten unas cartas firmadas que son enviadas a Casa Matriz garantizando el correcto funcionamiento del modelo de Control Interno SOX en el grupo. Éste modelo de Control Interno es supervisado por la Auditoría Interna (Contraloría) y un Revisor Externo.
Con el objetivo de elaborar y firmar la certificación SOX se deben realizar las siguientes actividades:

- ✓ Comprobar que han sido certificados por los responsables todos los controles SOX.

- ✓ Comprobar el alcance de las revisiones del modelo de control interno efectuadas por el Responsable de Controles SOX.

- ✓ El Modelo es evaluado anualmente por los Auditores Externos y por la Contraloría Interna.

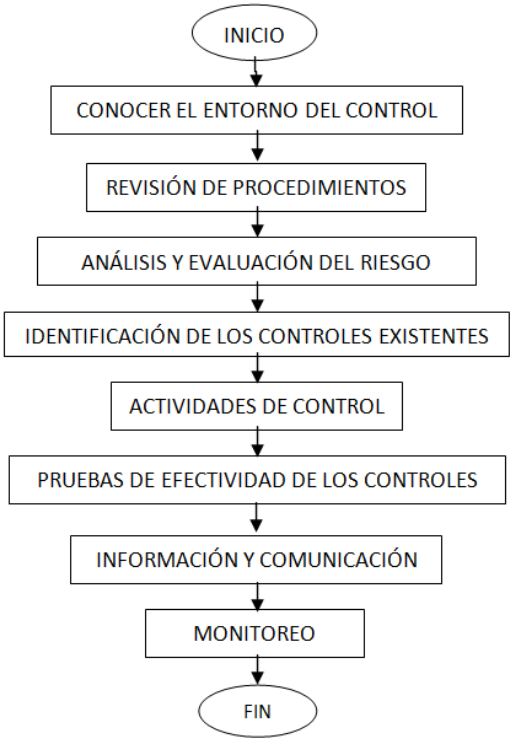
4. METODOLOGÍA

4.1 METODOLOGÍA DE IMPLEMENTACIÓN SCI

En éste proyecto se aplicó una metodología de implementación de un Sistema de Control Interno para la Gerencia de Producción de Helm Bank como se observa en la Figura 3. Fases de la Metodología de Implementación de SCI, mediante pasos organizados que consta de 8 fases y contempla los componentes necesarios de un Sistema de Control Interno:

- ✓ Conocer el Entorno de Control
- ✓ Revisión de procedimientos
- ✓ Análisis y evaluación del riesgo
- ✓ Identificación de los controles existentes
- ✓ Actividades de Control
- ✓ Pruebas de efectividad de los Controles
- ✓ Información y Comunicación
- ✓ Monitoreo

Figura 3. Fases de la Metodología de Implementación de SCI



Fuente Elaborado por el Autor

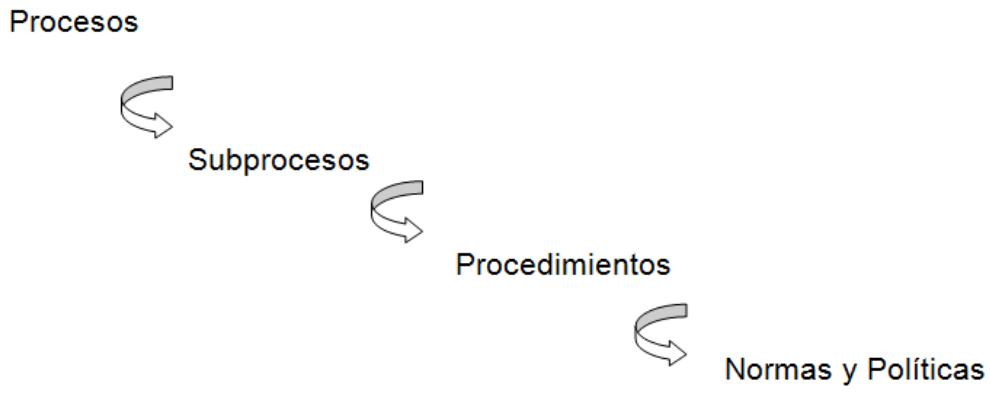
4.1.1 Conocer el entorno de control. El entorno de control establece la forma en la que una organización opera e influye en la manera de actuar de las personas. Marca la pauta del comportamiento en una organización, la disciplina, los valores éticos, la capacidad y estructura organizativa, la segregación de funciones y el desarrollo profesional, siendo la base de todos los demás componentes del control interno. Ésta fase aplica para la Gerencia de Producción de Helm Bank para conocer los roles y la funciones desempeñadas en cada actividad.

4.1.2 Revisión de procedimientos. En los procedimientos se dan los lineamientos para la gestión integral del proceso, que son de estricto cumplimiento para todos los Funcionarios de la Organización. Para la Gerencia de Producción como para la demás áreas de tecnología es necesario que existan Procedimientos dentro de cada Dirección, ya que éstos contienen normas y políticas que facilitan la realización de un trabajo de la manera más correcta y exitosa posible.

Como se observa en la Figura 4. Organización de Procesos en la Herramienta DocManager, el Banco Corpbanca dentro de su Modelo de Control Interno, contiene Procesos, Subprocesos, Procedimientos, Normas y Políticas, orientado a los lineamientos de cumplimiento en toda la organización.

Se revisó con cada Director de las áreas que los procedimientos existieran, estuvieran actualizados y publicados en la Herramienta DocManager y a su vez, estuvieran contenidos dentro de los procesos generales en el siguiente orden: Procesos, Subprocesos, Procedimientos, Normas y Políticas.

Figura 4. Organización de Procesos en la Herramienta DocManager

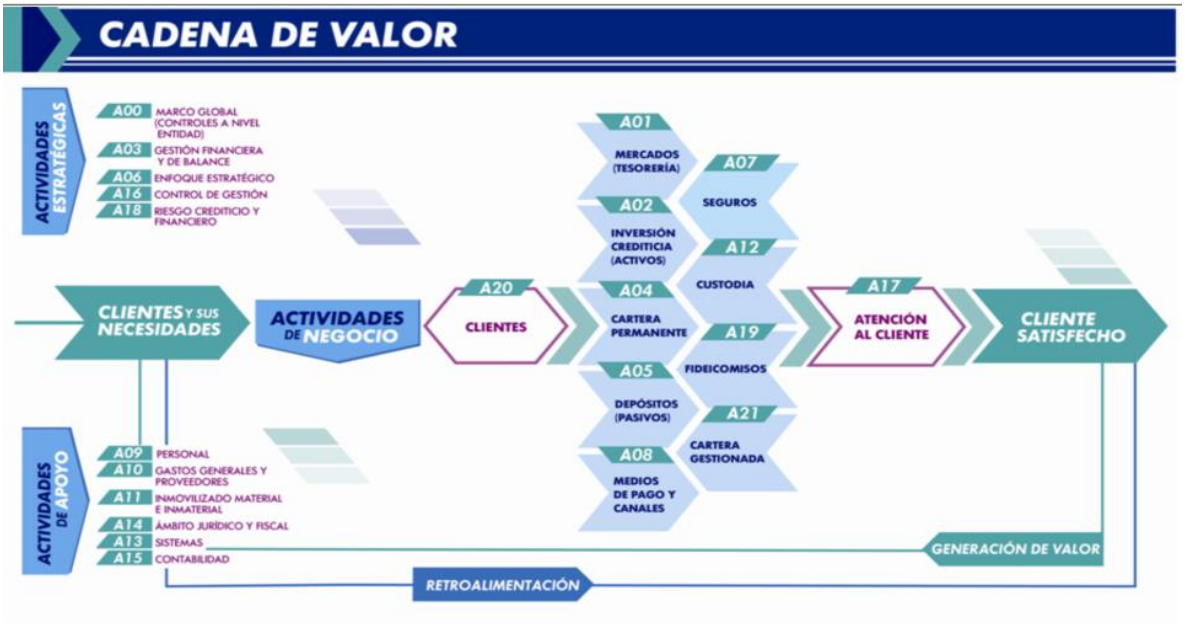


Fuente Elaborado por el Autor

En el banco unificado existen procesos generales, los procesos contienen subprocesos, los subprocesos contienen procedimientos y los procedimientos contienen las normas y políticas establecidas, de acuerdo a las actividades de Apoyo de la Cadena de Valor por cada área.

Como se aprecia en la Figura 5. Cadena de Valor Banco Unificado, cada Vicepresidencia debe ser identificada con una Letra y un Número para su reconocimiento. Igualmente todos los documentos de procesos (subprocesos, procedimientos, normas y políticas, formatos, manuales, anexos, entre otros) deben asociarse ó estar clasificados en la Cadena de Valor.

Figura 5. Cadena de Valor Banco Unificado



Fuente Banco Corpbanca Colombia.

Si se observa que hay funciones realizadas al interior de una Dirección que no se encuentren soportadas, deberá elaborarse un nuevo Subproceso y un nuevo procedimiento que contenga normas y políticas de esa función realizada siempre y cuando sean funciones repetitivas ó de alto impacto. Los Subprocesos y los Procedimientos también deben ser actualizados cuando haya nuevas directrices de la Superintendencia financiera ó por recomendación de los Entes de Control Internos y Externos.

4.1.3 Análisis y evaluación del riesgo. Esta fase de análisis y evaluación de riesgos es un proceso dinámico utilizado para identificar y evaluar los riesgos. La importancia de cada riesgo en el control interno se basa en su probabilidad de manifestación y en el impacto que puede causar en la organización.

A continuación se mencionan los pasos que se llevaron a cabo en el análisis y evaluación de riesgos en las 5 Direcciones de la Gerencia de Producción.

4.1.3.1 Entrevistas. Se realizaron entrevistas con los Directores y responsables de las áreas, buscando conocer la operación en aspectos tecnológicos como en los procesos críticos del día a día que ya se encuentran documentados en la Vicepresidencia de Tecnología, los cuales son soportados por las aplicaciones y la infraestructura tecnológica.

4.1.3.2 Evaluación de Riesgo. La evaluación de riesgos consiste en la identificación y el análisis de los riesgos relevantes y su probabilidad de ocurrencia, para esto se tuvo en cuenta las Tipologías de Riesgos que se encuentran mencionadas en el Cuadro 1. Tipologías de Riesgos y definidas en el *"Formato FT1494 Matriz de Riesgos y Controles SOX.xls"* de la Vicepresidencia de Riesgo, en los siguientes Niveles:

- ✓ Errores
- ✓ Fraude Externo
- ✓ Fraude Interno
- ✓ Tecnología
- ✓ Prácticas Comerciales
- ✓ Desastres
- ✓ Proveedores
- ✓ Recursos Humanos

Cuadro 1. Tipologías de Riesgos

Tipologias de Riesgos		
Nivel 1	**Nivel 2**	**Código de Riesgo (*)**
Errores	Errores en la Operativa	R11
	Incumplimiento de la normativa	R12
	Errores en la gestión y admon de cuentas con clientes	R13
	Incumplimiento de contratos con no clientes	R14
Fraude Externo	Otros fraudes externos	R21
	Violación de la Seguridad Informática	R22
	Uso Fraudulento de tarjetas	R23
	Robos y atracos	R24
Fraude Interno	Robos y fraudes	R31
	Actividades no autorizadas	R32
Tecnología	Tecnología	R41
Prácticas Comerciales	Prácticas Comerciales impropias	R51
	Política Comercial	R52
	Asesoramiento deficiente a clientes	R53
	Productos defectuosos	R54
	Trasgresión de instrucciones de clientes	R55
	Divulgación de información	R56
Desastres	Desastres y accidentes	R61
Proveedores	Proveedores	R71
Recursos Humanos	Gestión de Recursos Humanos	R81
	Incumplimiento de normativa legal	R82
	Discriminación, acosos	R83

(*) El código de la tipología de riesgo se completa con el tercer nivel de riesgo, que en última instancia proporciona una descripción más detallada del riesgo.

Fuente "Formato FT1494 Matriz de Riesgos y Controles SOX.xls". Banco Corpbanca Colombia.

A su vez el *"Formato FT1494 Matriz de Riesgos y Controles SOX.xls"* de la Vicepresidencia de Riesgo, contiene la descripción de los errores contables que hacen parte de la Tipología de Riesgos.

Como se observa a continuación en el Cuadro 2. Descripción de Errores Contables, los errores contables corresponden a omisiones o inexactitudes en los estados financieros de una entidad, por éste motivo deben estar contemplados en la evaluación del riesgo. En éste cuadro se realiza una descripción de los posibles errores contemplados dentro de la Organización.

Cuadro 2. Descripción de Errores Contables

Error	Descripción
Integridad	Error producido por no haberse registrado la operación.
Validez	Error producido porque se hayan registrado en los estados financieros del ejercicio operaciones que no son válidas, bien por no ser reales, bien por no contar con la debida autorización.
Corte de Operaciones	Error por existir operaciones que no se encuentren registradas en los estados financieros en el período correcto.
Registro	Error por existir operaciones registradas en los estados financieros con datos (importes, tipos, plazos, etc.) diferentes a los términos y condiciones de las transacciones.
Valoración	Error por existir activos, pasivos, derechos y compromisos que no están recogidos en los estados financieros con los importes correctos.
Presentación	Error por existir diferentes elementos de los estados financieros que puedan no estar correctamente clasificados, tanto en líneas del balance de situación o de la cuenta de pérdidas y ganancias, como en los desgloses de información.
Salvaguarda de activos	Error en los estados financieros por existir activos que no han sido adquiridos o no están en uso o pasivos que no se hayan incurrido y/o cancelado conforme a la autorización de la Dirección de la sociedad.
Incumplimiento	Error que se pone de manifiesto por el incumplimiento de la normativa aplicable y/o de las obligaciones adquiridas frente a los clientes en el curso de la operativa habitual y que puedan dar lugar a reclamaciones y por tanto posible pérdidas para la sociedad.

Fuente "Formato FT1494 Matriz de Riesgos y Controles SOX.xls". Banco Corpbanca Colombia.

Fue necesaria ésta evaluación de riesgos porque sobre ellos se generó un plan de implementación de los controles que garanticen un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

4.1.3.3 Determinar la Probabilidad de Ocurrencia. Teniendo la información de los riesgos presentados en los procesos críticos como resultado de las entrevistas de cada área y documentados para la Vicepresidencia de Tecnología, procedemos a clasificar los riesgos de acuerdo a su periodicidad y probabilidad de ocurrencia utilizando el *"Formato FT1494 Matriz de Riesgos y Controles SOX.xls"* de la Vicepresidencia de Riesgo.

El Cuadro 3. Probabilidad de Ocurrencia mencionado a continuación, representa la probabilidad de que se produzcan eventos de riesgo determinados ó el volumen de ocurrencia previsto para un periodo de tiempo dado, que puede ser clasificada en Alta, Media - Alta, Media, Media - Baja y Baja. Ésta probabilidad de ocurrencia fue necesaria dentro de la evaluación de riesgos:

Cuadro 3. Probabilidad de Ocurrencia

Probabilidad	Representa la probabilidad de que se produzcan eventos de riesgo determinados ó el volúmen de ocurrencia previsto para un período de tiempo dado	
PROBABILIDAD	**VALOR**	**DESCRIPCIÓN**
Alta	5	Ocurrencia semanal o superior (48 o más vecesa al año) o el proceso y/o la transacción se realiza mínimo cuarenta y ocho vez al año.
Media-Alta	4	Ocurrencia entre 1 y 4 veces al mes (12 - 47 veces al año) o el proceso y/o la transacción se realiza máximo cuarenta y site vez al año.
Media	3	Ocurrencia entre 1 y 4 veces al trimestre (4 - 11 veces al año) o el proceso y/o la transacción se realiza máximo once vez al año.
Media-Baja	2	Ocurrencia entre 1 y 3 veces al año o el proceso y/o la transacción se realiza máximo tres vez al año.
Baja	1	No se tiene experiencia de que se produzca o se produce con periodicidad superior a la anual ó el proceso y/o la transacción se realiza máximo una vez al año.

Fuente "Formato FT1494 Matriz de Riesgos y Controles SOX.xls". Banco Corpbanca Colombia.

4.1.3.4 Análisis del impacto. Se realizó un análisis de impacto para medir la afectación negativa que podría causar en la organización, pues las consecuencias de no mitigar éstos riesgos a tiempo pueden ser de tipo financiero y es precisamente lo que la Ley Sox precisa evitar. Para realizar ésta actividad fue utilizado el Cuadro 4. Análisis de Impacto, el cual determina la severidad con que se plasman los eventos de riesgo cuando se producen. La puntuación representa una cuantificación económica.

En ésta etapa se determina la severidad de los eventos de riesgo cuando se producen. La puntuación de los valores mencionados a continuación representa una cuantificación económica. El análisis de impacto se encuentra definido en el *"Formato FT1494 Matriz de Riesgos y Controles SOX.xls"* de la Vicepresidencia de Riesgo. El impacto se clasifica como Alto, Medio - Alto, Medio, Medio - Bajo y Bajo:

Cuadro 4. Análisis de Impacto

Impacto	Determinación de la severidad con que se plasman los eventos de riesgo cuando se producen. La puntuación representará una cuantificación económica.

IMPACTO	VALOR	DESCRIPCIÓN
Alto	5	Pérdidas mayores a $2.500MM o el importe promedio de las transacciones superan la cuantía indicada.
Medio-Alto	4	Pérdidas mayores a $250MM y menores a $2.500MM o el importe promedio de las transacciones se encuentra dentro del rango indicadono.
Medio	3	Pérdidas mayores a $50MM y menores a $250MM o el importe promedio de las transacciones se encuentra dentro del rango indicadono.
Medio-Bajo	2	Pérdidas mayores a $7,5MM y menores o iguales a $50MM o el importe promedio de las transacciones se encuentra dentro del rango indicadono.
Bajo	1	Pérdidas inferiores a $7,5MM o el importe promedio de las transacciones no superan los $7,5MM.

Fuente "Formato FT1494 Matriz de Riesgos y Controles SOX.xls". Banco Corpbanca Colombia.

Como resultado de éste análisis de impacto fue posible listar los riesgos empezando por los que se han categorizado como de alto impacto y alta probabilidad de ocurrencia, sin dejar de vista los de bajo impacto. Ésta información es la base para elaborar un Control por cada uno de los Riesgos encontrados.

4.1.4 Identificación de los controles existentes. En esta fase se indagó con las 5 Direcciones de la Gerencia de Producción respecto a los controles existentes para el desarrollo de sus actividades. Aquí se revisa que los controles estén soportados en los Subprocesos y en los procedimientos y además se encuentren actualizados y sean suficientes para todas las tareas realizadas en las áreas. Los controles se consideran suficientes cuando tienen una cobertura amplia en cuanto a las funciones realizadas por la Dirección y además respaldan un evento de riesgo detectado, pues cada control que se realice dentro de la organización debe estar de acuerdo con el riesgo que previene.

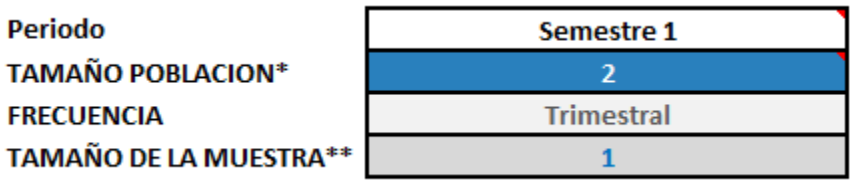
4.1.5 Actividades de control. Las actividades de control conforman un elemento fundamental de los elementos de control interno. Estas actividades están orientadas a minimizar los riesgos identificados durante el proceso de evaluación de riesgos y que dificulten la realización de los objetivos generales de la

organización, asegurando que se llevan a cabo los lineamientos establecidos por parte de cada funcionario encargado dentro de su rol.

En ésta fase se redactaron los Controles correspondientes a cada evento de riesgo detectado en la Gerencia de Producción, ya que cada riesgo debe tener un control establecido.

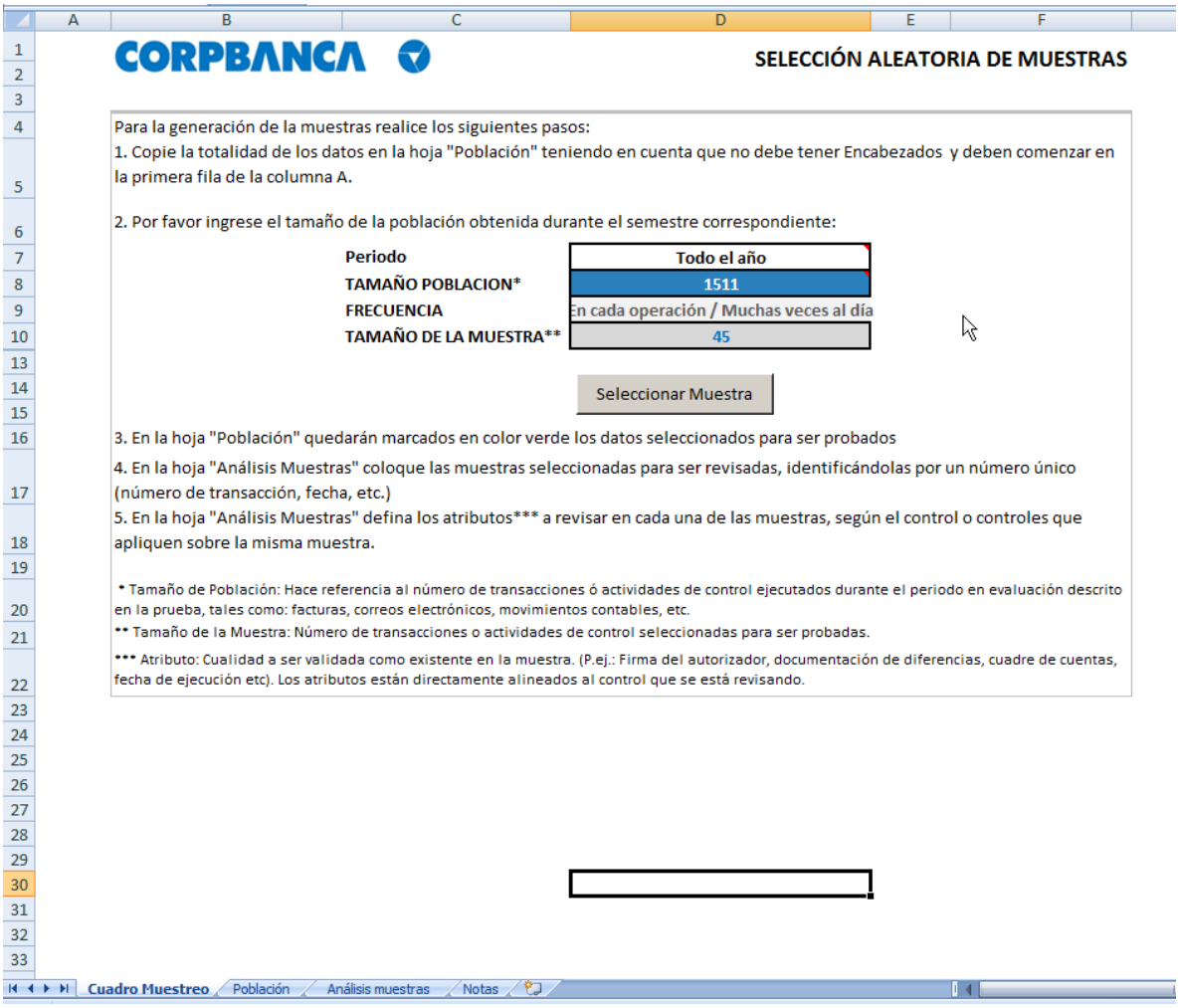
4.1.6 Pruebas de efectividad de los controles. Como se observa en la Figura 6. Selección aleatoria de la muestra - Formato FT1552 Prueba Controles MCI-SOX y Figura 7. Formato de Pruebas de Control Sox - FT1552 - Hoja Cuadro de Muestreo, las pruebas de efectividad de los Controles garantizan el cumplimiento de los mismos con base en la existencia de las evidencias. Consiste en seleccionar la periodicidad del control, el tamaño de la población, la frecuencia y el tamaño de la muestra anual. Para ésta actividad se corren macros en Excel que realizan una selección aleatoria de acuerdo a un cuadro de muestreo previamente diligenciado y una población. Estas macros están contenidas en el "Formato *FT1552 Prueba Controles MCI-SOX.xls"* de la Vicepresidencia de Riesgo.

Figura 6. Selección aleatoria de la muestra - Formato FT1552 Prueba Controles MCI-SOX



Fuente Banco Corpbanca Colombia.

Figura 7. Formato de Pruebas de Control Sox - FT1552 - Hoja Cuadro de Muestreo



Fuente Banco Corpbanca Colombia.

El tamaño de la muestra corresponde al número de transacciones o actividades de control seleccionadas para ser probadas. Existe un cuadro de frecuencias en el "*Formato FT1552 Prueba Controles MCI-SOX.xls"* de la Vicepresidencia de Riesgo, para seleccionar el tamaño de la muestra.

Cuadro 5. Frecuencias para seleccionar el tamaño de la muestra

Frecuencia	Todo el año	Semestre 1	Semestre 2
En cada operación	45	23	22
Diaria	25	13	12
Semanal	8	4	4
Quincenal	6	3	3
Mensual	3	2	1
Trimestral	2	1	1
Semestral	2	1	1
Anual	1	0	1
Controles Automáticos	2	1	1

Fuente "Formato FT1552 Prueba Controles MCI-SOX.xls". Banco Corpbanca Colombia.

En una de las hojas en Excel del *"Formato FT1552 Prueba Controles MCI-SOX.xls"* de la Vicepresidencia de Riesgo, también están contenidas las frecuencias asimilables disponibles a seleccionar, de acuerdo con el número de veces que se ha ejecutado el control durante el periodo a certificar. Esto para efecto de las pruebas que se deben realizar.

El Cuadro 5. Frecuencias para seleccionar el tamaño de la muestra y el Cuadro 6. Frecuencias asimilables de los Controles, hacen referencia a los controles clasificados como "En cada operación" se asemejan a la frecuencia de control más próxima. Estas frecuencias asimilables de los controles, son fundamentales para la entrega de evidencias.

Cuadro 6. Frecuencias asimilables de los Controles

Los controles clasificados como "En cada operación" se asemejarán a la frecuencia de control más próxima:

Frecuencias asimilables:	N° de veces que se ha ejecutado el control en el año	N° de veces que se ha ejecutado el control en el semestre
Muchas veces al día / En cada Operación	>365	_>183
Diario	365 >_ y > 100	183_>y >50
Semanal	100 _>y >24	50_>y >12
Mensual	24 _>y >6	12_> y >3
Trimestral	6_>y >2	3_>y >1
Anualmente	1	1

Fuente "Formato FT1552 Prueba Controles MCI-SOX.xls". Banco Corpbanca Colombia.

En el "*Formato FT1552 Prueba Controles MCI-SOX.xls"* de la Vicepresidencia de Riesgo, existen 3 tipos de evaluación válidos para realizar las pruebas de efectividad, éstas son: Auto-evaluación, Pruebas cruzadas ó No aplica pruebas, como se puede apreciar en el Cuadro 7. Tipo de Evaluación de Controles.

Auditoría Auto-evaluación: Pruebas de efectividad que realizan los propios responsables del control ó personal de la misma área.

Auditoría pruebas cruzadas: Pruebas realizadas por personal diferente al responsable del control y sin ningún tipo de relación jerárquica con éste (Personas de otra área).

No aplica pruebas: Se utiliza sólo si durante el periodo a certificar, no se presentó operativa relacionada con el control establecido.

Cuadro 7. Tipo de Evaluación de Controles

Tipo evaluación
Auto-evaluación 2: En este caso, las pruebas de efectividad las realizan los propios responsables del control ó personal de la misma área.
Pruebas cruzadas: En este caso, las pruebas cruzadas son realizadas por personal diferente al responsable del control y sin ningún tipo de relación jerárquica con éste. (Personas de otra área)
No aplica: Utilizar sólo si durante el período a certificar, **no se presentó operativa** relacionada con el control establecido.

Fuente "Formato FT1552 Prueba Controles MCI-SOX.xls". Banco Corpbanca Colombia.

De acuerdo al resultado de la selección se verifica que para esa operación ó fecha exista una evidencia y además esté completa y no haya sido alterada. Finalmente se registra en una hoja del formato de prueba de efectividad el resultado. Si almenos una de éstas muestras aleatorias seleccionadas no tiene evidencia ó está incompleta, el control se considera como No Efectivo.

Las pruebas de efectividad de los controles internos están a cargo del Gerente, el Director del Área, ó de la persona que sea delegada por ellos.

4.1.7 Información y comunicación. La información es necesaria para que la Entidad pueda llevar a cabo sus responsabilidades de control interno y soportar el logro de sus objetivos. La comunicación interna es el medio por el cual la información se difunde a través de toda la organización que fluye en sentido ascendente, descendente y en todos los niveles de la organización. Es responsabilidad de cada Jefe de las Direcciones de la Gerencia de Producción hacer extensiva la información de los Controles vigentes y aquellos que fueron actualizados ó eliminados si fuera el caso, a su grupo de trabajo.

4.1.8 Monitoreo. Las Evaluaciones continuas y las evaluaciones independientes o una combinación de ambas se utilizan para determinar si cada uno de los 5 componentes del Control Interno están presentes y funcionan adecuadamente. Éste monitoreo se realiza por parte de los Entes de Control Internos y Externos

cuando ha finalizado el proceso de certificación por el Gerente de Producción como por los demás Directivos responsables en la Organización.

5. DESARROLLO DEL PROYECTO

5.1 IMPLEMENTACIÓN DEL SISTEMA DE CONTROL INTERNO EN LA GERENCIA DE PRODUCCIÓN

En éste capítulo se aprecia la aplicación de la metodología mencionada en el capítulo 4, respecto a la implementación de un Sistema de Control Interno para la Gerencia de Producción de Helm Bank.

5.1.1 Periodo de certificación. Debido a que Helm Bank no había participado antes en un proceso de Certificación SOX, el periodo de revisión y auditoría fue el comprendido entre el 01 de Enero 2014 al 31 de Diciembre de 2014 y fue certificado el día 10 de Marzo de 2015.

5.1.2 Capacitaciones y lineamientos. Como parte de la implementación del Sistema de Control Interno en la Gerencia de Producción de Helm Bank a partir del 08 de Octubre de 2014, se efectuó una reunión citada por los Asesores SOX de la Gerencia de Riesgo Operativo y Seguridad, con las 5 Direcciones que forman parte de la Gerencia de Producción, el Jefe de Aseguramiento de Calidad y demás personas que formamos parte del equipo de trabajo seleccionado para el proceso de Certificación SOX, con el fin de dar a conocer la nueva directriz en cuanto al Cumplimiento del Modelo de Control Interno para las diferentes áreas del Banco a partir de la Fusión Legal.

En ésta reunión se realizó una presentación respecto a:

- ✓ Sistema de Control Interno (SCI)
- ✓ Estructura del Modelo SCI – SOX
- ✓ Ley SOX
- ✓ Perímetro SOX
- ✓ Modelo de certificación SCI – SOX
- ✓ Evaluación MCI SOX

Luego de ésta fecha y hasta Febrero de 2015, se realizaron algunas reuniones de entendimiento, capacitación y asesoría por parte de la Gerencia de Riesgo Operativo y Seguridad a las áreas de tecnología, brindando apoyo en todo el proceso de Certificación MCI – SOX.

De acuerdo a la "Circular Externa 038" de 2009 emitida por la Superintendencia Financiera de Colombia, el "Modelo Corporativo de Control Interno" se

implementó como la metodología corporativa Sarbanes-Oxley (SOX). Mediante este esquema se definen los procesos transversales, desarrollados de principio a fin por cada tema o producto, realizando la identificación y definición simultánea de los riesgos y controles.

Para el mes de Febrero 2015, los Asesores SOX de la Gerencia de Riesgo Operacional y Seguridad realizan entrega de una Guía de certificación MCI-SOX a las áreas de tecnología. Ésta guía contiene los siguientes puntos a tener en cuenta:

- ✓ Fecha límite de Certificación por parte de las Áreas de Tecnología
- ✓ Responsables de la Certificación
- ✓ Diligenciamiento de documento de Certificación
- ✓ Diligenciamiento de Matriz SOX

Igualmente entregan a las Áreas de Tecnología 2 documentos que hacen parte de la certificación final, los cuales son de uso obligatorio para todos los controles a certificar:

- ✓ Formato FT1552 Prueba Controles MCI-SOX
- ✓ Formato FT1494 Matriz de Riesgos y Controles SOX

5.1.3 Matriz de Riesgos y Controles Sox. La Matriz de Riesgos y Controles SOX está compuesta por los siguientes campos a diligenciar en su totalidad y consta de 3 secciones:

- ✓ Información de Controles
- ✓ Evaluación de Controles
- ✓ Proceso de Certificación

A continuación se describe la información contenida en cada uno de éstas secciones que componen la Matriz de Riesgos y Controles SOX:

5.1.3.1 Información de Controles. Los campos correspondientes a la información de los controles son:

- ✓ Código Entidad
- ✓ Entidad
- ✓ Código Actividad
- ✓ Actividad
- ✓ Proceso
- ✓ Código Subproceso
- ✓ Nombre Subproceso

- ✓ Código Tipología Riesgos
- ✓ Riesgo
- ✓ Evento de Riesgo
- ✓ Tipo de Riesgo
- ✓ Número de Control
- ✓ Actividad de Control
- ✓ Tipo Evidencia
- ✓ Descripción Evidencia
- ✓ Responsable Control
- ✓ Puesto Responsable
- ✓ Categoría
- ✓ Frecuencia
- ✓ Tipología
- ✓ Naturaleza
- ✓ Aplicación
- ✓ Importancia
- ✓ Efectividad Diseño
- ✓ Efectividad Funcionamiento
- ✓ Comentario Ef. Diseño
- ✓ Comentario Ef. Funcionamiento
- ✓ Error Contable (*Hace referencia a cómo se puede ver afectado el Grupo Financiero contablemente si no se cumplen los controles propuestos*).

5.1.3.2 Evaluación de Controles. Los campos correspondientes a la evaluación de los controles son:

- ✓ Frecuencia de la Prueba
- ✓ Semestre auditado
- ✓ Tipo de Evaluación
- ✓ Tamaño de la muestra anual
- ✓ Tamaño de la muestra del periodo de certificación
- ✓ Repetición de la muestra tomada
- ✓ Resultado de la Prueba
- ✓ Observaciones

5.1.3.3 Proceso de Certificación. Los campos correspondientes al proceso de certificación de los controles son:

- ✓ Nombre Gerente / Jefe Responsable
- ✓ Cargo
- ✓ Tipo de Certificación
- ✓ Fecha de Certificación
- ✓ Estado

✓ Código de Control

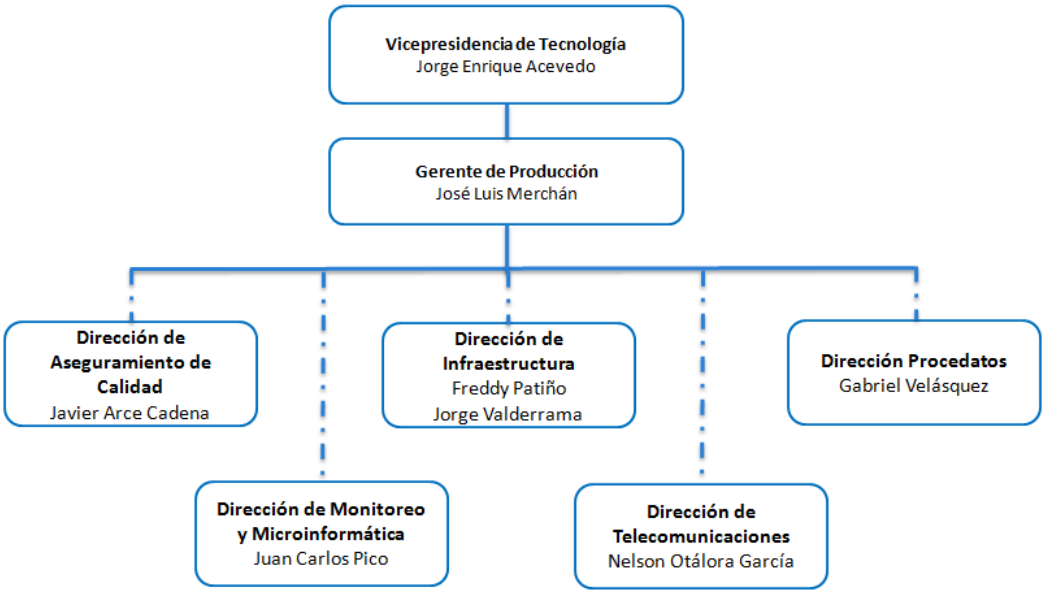
A partir de éste punto cada una de las Direcciones de la Gerencia de Producción que a su vez forman parte de la Vicepresidencia de Tecnología, es responsable del cumplimiento de certificación de controles del Modelo de Control Interno (MCI) SOX para todo el Año 2014.

5.2 DIRECCIONES DE TECNOLOGÍA QUE CONFORMAN LA GERENCIA DE PRODUCCIÓN

Dentro de la Vicepresidencia de Tecnología de Helm Bank se encuentra la Gerencia de Producción también conformada por 5 Direcciones de Tecnología. En la Figura 8. Organigrama de la Gerencia de Producción de Helm Bank y sus Direcciones, se puede apreciar la jerarquía de la Vicepresidencia de Tecnología y sus representantes.

- ✓ Dirección de Aseguramiento de Calidad
- ✓ Dirección de Infraestructura
- ✓ Dirección de Monitoreo y Microinformática
- ✓ Dirección del Centro de Procesamiento de Datos
- ✓ Dirección de Telecomunicaciones

Figura 8. Organigrama de la Gerencia de Producción de Helm Bank y sus Direcciones



Fuente Elaborado por el Autor

5.3 RESPONSABILIDADES DENTRO EL PROCESO DE IMPLEMENTACIÓN SCI

Por temas de Confidencialidad de la Información el Trabajo de Grado fue realizado de manera individual por el estudiante de la Especialización en Seguridad Informática, sin embargo, dentro de la Organización éste hizo parte del grupo de personas delegadas para realizar la implementación del SCI en la Gerencia de Producción.

El aporte que se realizó dentro de éste proyecto de Certificación SOX estuvo centrado en las siguientes actividades y responsabilidades:

- ✓ Realizar planeación para la implementación de una Sistema de Control Interno en la Gerencia de Producción.

- ✓ Levantamiento de información en las 5 Direcciones de la Gerencia de Producción.

- ✓ Consolidar la información de riesgos y eventos de riesgo relevantes en toda la Gerencia de Producción para clasificarlos por su frecuencia.

- ✓ Revisión de Procesos, Subprocesos y Procedimientos existentes en las 5 Direcciones de la Gerencia de Producción y a su vez verificar que éstos se encuentren publicados en la Base de Conocimiento de Helm Bank, para establecer si existen normas y políticas al interior de cada Dirección, si éstas se encuentren documentadas y si están siendo cumplidas en cada actividad realizada por parte del funcionario encargado.

- ✓ Reunión con un Asesor de la Gerencia de Procesos para revisar que los Procedimientos de cada área se encuentren correctamente organizados dentro de los Procesos y Subprocesos generales y a su vez, conocer los códigos de Proceso, códigos de Subproceso y códigos de Tipología de Riesgos.

- ✓ Revisión de la Cadena de Valor a nivel de la Vicepresidencia de Tecnología para conocer y verificar el código de actividad de apoyo del Área de Tecnología.

- ✓ Construir y redactar los eventos de Riesgo de acuerdo a los procedimientos existentes en las 5 Direcciones de la Gerencia de Producción y al Modelo de Control Interno recomendado por la Gerencia de Riesgo Operativo y Seguridad. En ésta actividad se redacta un total de 20 Eventos de Riesgo para toda la Gerencia de Producción.

- ✓ Construir y redactar las Actividades de Control de las 5 Direcciones de la Gerencia de Producción, de acuerdo al Modelo de Control Interno recomendado y suministrado por la Gerencia de Riesgo Operativo y Seguridad. En ésta actividad se redacta un total de 20 Actividades de Control para toda la Gerencia de Producción, ya que cada evento de riesgo debe tener un control establecido.

- ✓ Garantizar que por cada Dirección se realizara la Aprobación de los Eventos de riesgo, las Actividades de Control y en general a la Matriz SOX.

- ✓ Realizar auditorías cruzadas con 2 de las 5 Direcciones de la Gerencia de Producción (Dirección de Monitoreo y Microinformática y Dirección de Telecomunicaciones).

- ✓ Recibir la visita de Auditoría Interna - Evaluación de los controles SOX y dar respuesta a las solicitudes de información requerida.

- ✓ Verificar en el Servidor documental de la Gerencia de Producción, la existencia de las evidencias de los controles por cada una de las Direcciones de la Gerencia de Producción, de acuerdo a su frecuencia mencionada en la actividad de control.

- ✓ Ejecutar Pruebas de Controles Sox, las cuales consisten en revisar la periodicidad del control, el tamaño de la población, la frecuencia y el tamaño de la muestra anual. Luego realizar un análisis de las muestras para ejecutar las pruebas de Controles SOX. Para ésta actividad se corren algunas macros que realizan una selección aleatoria de acuerdo a un cuadro de muestreo y una población, y finalmente se realiza un análisis de las muestras mencionando si la evidencia existe y está completa.

- ✓ Verificar los resultados de las pruebas de Controles SOX en las 5 Direcciones de la Gerencia de Producción y mencionar la conclusión de la prueba, la cual es “Efectivo ó No Efectivo”. En caso de que éste resulte No Efectivo, se debe redactar el plan de acción. En los resultados de las pruebas se encontraron 2 Controles No Efectivos para la Dirección de Infraestructura.

- ✓ Realizar Auditoría Auto-evaluación para la Dirección de Aseguramiento de Calidad. En ella se revisa que la documentación de las Solicitudes Pruebas y la documentación de los Cambios a instalar en Producción revisados por el Área de Aseguramiento de Calidad, cumplan con todo lo establecido en los procedimientos respectivos.

- ✓ Diligenciar completamente el Formato FT1552 - Prueba de controles SOX por cada una de las Actividades de Control de las Direcciones de la Gerencia de

Producción, en la que se conservan las muestras aleatorias y el análisis de las muestras.

- ✓ Diligenciar completamente la Matriz SOX Final. Ésta consistió en consolidar toda la información correspondiente a los procesos, subprocesos, riesgos, eventos de riesgos, actividades de control y frecuencia, tipo, descripción y ruta de las evidencias, responsables de los controles, evaluación de los controles de acuerdo al resultado de las pruebas de Controles Sox con su respectivo análisis y certificación final por parte de la Gerencia de Producción.

- ✓ Verificar el diligenciamiento y firma de la Certificación SOX por parte de la Gerencia de Producción.

- ✓ Hacer entrega de la Matriz SOX Final, Certificación SOX y Formatos FT1552 - Prueba de controles SOX diligenciados, a la Gerencia de Procesos Operativos y Seguridad.

- ✓ Realizar seguimiento trimestral al cumplimiento del total de los Controles Propuestos en la Gerencia de Producción.

De estas responsabilidades mencionadas es necesario resaltar las 5 más significativas:

5.3.1 Planeación y levantamiento de información. Se realiza una planeación para la implementación de una Sistema de Control Interno en la Gerencia de Producción, para establecer el alcance y las fechas estimadas de certificación de acuerdo a la fecha límite informada por la Gerencia de Riesgo Operativo y Seguridad.

Se efectúa un levantamiento de información con el fin de identificar y analizar los riesgos y eventos de riesgo relevantes presentados en las 5 Direcciones de la Gerencia de Producción. Para esto fue necesario realizar constantes reuniones con los Jefes de éstas Direcciones y otros funcionarios que tienen tareas específicas en cada área y luego se procede a consolidar la información.

5.3.2 Identificación y Evaluación de Riesgos. Los riesgos se identifican en los procesos y deben describirse dentro de los sub-procesos o procedimientos de cada Dirección. Cada Dirección se enfrenta a diversos riesgos internos y externos que deben ser evaluados. La evaluación de riesgos consistió en la identificación y el análisis de los riesgos relevantes y probabilidad de ocurrencia, para esto se tuvo en cuenta las siguientes tipologías de riesgos:

- ✓ Desastres
- ✓ Errores
- ✓ Fraude Externo
- ✓ Fraude Interno
- ✓ Prácticas Comerciales
- ✓ Proveedores
- ✓ Recursos Humanos
- ✓ Tecnología

De ésta manera fue posible construir y redactar los eventos de riesgo. En ésta actividad se redacta un total de 20 Eventos de Riesgo para toda la Gerencia de Producción.

5.3.3 Construcción de Actividades de Control. Las actividades de control son mecanismos que permiten a la Dirección administrar (mitigar) los riesgos identificados durante el proceso de Evaluación de Riesgos y asegurar que se llevan a cabo los lineamientos establecidos por parte del funcionario encargado.

Los controles indican ejecución de una acción y por lo tanto deben empezar con un verbo en infinitivo. Para la descripción de los controles se tuvo en cuenta los siguientes factores y el orden de acuerdo a capacitación recibida:

- ✓ Acción (Que)
- ✓ Naturaleza: manual, automática o semiautomática.
- ✓ Cuándo - Frecuencia del control: (En cada operación, semanal, mensual, diaria, etc.)
- ✓ Quién valida la acción (Cargo)
- ✓ Qué se hace (Explica el objetivo del control)
- ✓ Tipología (Previo ó posterior)
- ✓ Ampliación de la tipología (Indica previo a que o posterior a que se realiza)
- ✓ Campo Fijo (Incluir la palabra: “mediante”)
- ✓ Cómo se hace (indicar cargo del generador de la operación)
- ✓ Campo Fijo (Incluir la frase: “dejando como evidencia”)
- ✓ Descripción de la evidencia
- ✓ Campo Fijo (Incluir la frase: “que se conserva en”)
- ✓ Lugar físico donde se conserva la evidencia
- ✓ Que hacer en caso de incidencia ó inconsistencia

De ésta manera fue posible construir y redactar las Actividades de Control. En ésta actividad se redacta un total de 20 Actividades de Control para toda la Gerencia de Producción.

Fue necesario garantizar que por cada Dirección se realizara la aprobación de los Eventos de riesgo, las Actividades de Control y en general la Matriz de Riesgos y Controles SOX.

5.3.3.1 Eventos de Riesgo y Actividades de Control. A continuación se presentan los Eventos de Riesgo y las Actividades de Control que se elaboraron y fueron aprobadas por cada una de las Direcciones que forman parte de la Gerencia de Producción:

Total de Eventos de Riesgos para la Gerencia de Producción: **20**
Total Actividades de Controles para la Gerencia de Producción: **20**

Dirección de Aseguramiento de Calidad

Cantidad de Riesgos detectados y Controles elaborados: **5**

Proceso: P03 - Desarrollo y Evolución de Aplicaciones
Código de Subproceso: SH1141
Nombre Subproceso: Seguimiento al desarrollo y/o modificación del sistema de infraestructura (y aplicaciones)
Código Tipología de Riesgos: R4105
Riesgo: Riesgo en la instalación de cambios en producción
Evento de Riesgo: Riesgo de Tecnología al avanzar cambios Emergentes, Estándar y Nocturnos a ejecutar en Producción cuando no se han realizado pruebas funcionales ó técnicas en ambientes previos, no han sido Autorizados, no tienen un cronograma de actividades y plan de reverso, no cuentan con evidencias de pruebas y a su vez no tienen un Correo ó Mantis del Usuario solicitante.
Actividad de Control: Validar y garantizar en cada Cambio por parte del Analista - Administrador de Cambios, que se cumpla con el Procedimiento de Cambios a Producción por parte de las Áreas de Tecnología, mediante la revisión de los requisitos indicados en el procedimiento, dejando como evidencia ésta misma documentación que se conserva en la Herramienta.
Número de Control: C01
Código de Control: A13SH1141R4105C01

Proceso: P03 - Desarrollo y Evolución de Aplicaciones
Código de Subproceso: SH1142
Nombre Subproceso: Pruebas de aceptación en aplicaciones ó cambios de infraestructura
Código Tipología de Riesgos: R4105

Riesgo: Mal funcionamiento de los sistemas de información por incorrecta o insuficiente fase de pruebas funcionales sobre el software.
Evento de Riesgo: Riesgo de Tecnología por mal funcionamiento de los sistemas de información por incorrecta o insuficiente fase de pruebas funcionales sobre el software, debido a que las Pruebas de Área en QA son incorrectas, incompletas, mal aplicadas ó se ha mal interpretado el resultado, ó por certificar pruebas por la modalidad de Visto Bueno cuando no se han realizado pruebas funcionales por parte de los Analistas de Pruebas de QA sino por el Usuario Final ó personas Desarrollo de la Gerencia de Tecnología del Negocio y Proveedores.
Actividad de Control: Realizar manualmente un cubrimiento total de las pruebas funcionales a las aplicaciones críticas (Helm Tesorería, OpenCard, Phoenix, Canales electrónicos) por parte del Analista de QA, además de la ejecución total del deck que contiene los casos de prueba elaborados, previo el análisis de la documentación mínima requerida en el Procedimiento de Pruebas y del conocimiento del alcance de las pruebas, mediante la elaboración de una planeación, dejando como evidencia los documentos soportes del Proceso, que se conservan en un servidor documental de QA por cada una de las Solicitudes de Pruebas radicadas en la herramienta. En caso de inconsistencias ó hallazgos presentados, se informa al Analista ó Subgerente de la Gerencia de Tecnología del Negocio para verificar las pruebas realizadas ó el ambiente de pruebas, de ser necesario. Si amerita, se genera un nuevo ciclo de pruebas.
Número de Control: C01
Código de Control: A13SH1142R4105C01

Proceso: P03 - Desarrollo y Evolución de Aplicaciones
Código de Subproceso: SH1142
Nombre Subproceso: Pruebas de aceptación en aplicaciones ó cambios de infraestructura
Código Tipología de Riesgos: R4105
Riesgo: Mal funcionamiento de los sistemas de información por incorrecta o insuficiente fase de pruebas funcionales sobre el software.
Evento de Riesgo: Riesgo de Tecnología por mal funcionamiento de los sistemas de información por incorrecta o insuficiente fase de pruebas funcionales sobre el software, debido a que las Pruebas de Área en QA son incorrectas, incompletas, mal aplicadas ó se ha mal interpretado el resultado, ó por certificar pruebas por la modalidad de Visto Bueno cuando no se han realizado pruebas funcionales por parte de los Analistas de Pruebas de QA sino por el Usuario Final ó personas Desarrollo de la Gerencia de Tecnología del Negocio y Proveedores.
Actividad de Control: Verificar que cada Solicitud de Pruebas radicada en ClearQuest por el Analista ó Subgerente de la Gerencia de Tecnología del Negocio, cumpla con los documentos definidos en el procedimiento de pruebas, dejando como evidencia la Certificación de Usuario, la Certificación de Desarrollos y la Certificación de Pruebas de QA por Modalidad de Visto Bueno, emitida por el Analista de Pruebas de QA. En caso de inconsistencias de la documentación ó

inconsistencias en la ruta branch que contiene los componentes, se devuelve al Analista ó Subgerente de la Gerencia de Tecnología del Negocio para que sea revisada.
Número de Control: C02
Código de Control: A13SH1142R4105C02

Proceso: P03 - Desarrollo y Evolución de Aplicaciones
Código de Subproceso: SH1142
Nombre Subproceso: Pruebas de aceptación en aplicaciones ó cambios de infraestructura
Código Tipología de Riesgos: R1102
Riesgo: Riesgo de errores en el Control de Versiones
Evento de Riesgo: Riesgo de que no exista un control de versiones y puedan pasar desarrollos entregados a producción que no han sido probados en ambientes previos.
Actividad de Control: Garantizar manualmente y para cada solicitud de pruebas por parte del Analista del Área Técnica de QA, que se realice el respectivo versionamiento en Subversión que contenga los componentes instalados en ambiente previo de QA y que fueron probados tanto por los Analistas de Pruebas como por los Usuarios, dejando como evidencia una ruta tags en la Certificación de pruebas emitida por el Analista de Pruebas ó Analista Técnico. Ésta evidencia se encuentra en Subversión para cada aplicativo con rutas branch y rutas tags y la Certificación de QA en el servidor documental.
Número de Control: C01
Código de Control: A13SH1142R1102C01

Proceso: P06-Gestión de la seguridad física y lógica
Código de Subproceso: SH1121
Nombre Subproceso: Administración de usuarios, accesos y perfiles de los sistemas y aplicaciones
Código Tipología de Riesgos: R1102
Riesgo: Errores en la operativa (entrada datos, duplicidades, retrasos, caja, etc.)
Evento de Riesgo: Riesgo de errores en la operativa debido a la no ejecución del (Script o Spufi) por falta de correos de autorización o por la falta de efectividad en la depuración de perfiles.
Actividad de Control: Validar y garantizar en cada Cambio por parte del Analista - Administrador de Cambios, que se cumpla con el Procedimiento de Cambios a Producción por parte de las Áreas de Tecnología, mediante la revisión de los requisitos indicados en el procedimiento, dejando como evidencia ésta misma documentación que se conserva en la Herramienta.
Número de Control: C01
Código de Control: A13SH1121R1102C01

Dirección de Infraestructura

Cantidad de Riesgos detectados y Controles elaborados: 4

Proceso: P04 - Mantenimiento de Aplicaciones e Infraestructura
Código de Subproceso: SH1150
Nombre Subproceso: Seguimiento al control de inventario de Software y Hardware
Código Tipología de Riesgos: R1111
Riesgo: Deficiencias en inventarios
Evento de Riesgo: Riesgo de errores generados por un inadecuado control de inventarios lo que puede conducir a la obsolescencia del hardware o software base "Sistema operativo" y ausencia de soporte por parte de los fabricantes.
Actividad de Control: Validar manualmente con frecuencia Trimestral por parte del Subgerente y/o analista, que tengan plataforma de Hardware a su cargo el inventario de activos tecnológicos previo a la salida de obsolescencia, mediante confrontar archivo de inventario en Excel contra los activos físicos (Servidores pertenecientes al Banco Corpbanca - Helm correspondientes a los Datacenter de los Edificios Calle 27 piso 10, Floresta I, Floresta II y DRP Comware). Garantizando la actualización del inventario de activos tecnológicos para minimizar el riesgo de obsolescencia de estos. Dejando como evidencia Archivo de inventario en Excel "Nombre Archivo" que se conservan en carpeta compartida en SharePoint, en caso de inconsistencias se genera un correo al gerente de producción notificando la inconsistencia.
Número de Control: C01
Código de Control: A13SH1150R1111C01

Proceso: P04 - Mantenimiento de Aplicaciones e Infraestructura
Código de Subproceso: SH1801
Nombre Subproceso: Actualización, Depuración y Modificación de Datos en Aplicaciones
Código Tipología de Riesgos: R4101
Riesgo: Funcionamiento inadecuado de la aplicación software
Evento de Riesgo: Deterioro del rendimiento en las aplicaciones e indisponibilidad del servicio, por falta de labores de mantenimiento y depuración de las bases de datos Corporativas de Aplicaciones Core (Phoenix, OpenCard, Helm Tesorería, Credismart, Datawarehouse).
Actividad de Control: Ejecutar manual y automáticamente con frecuencia mensual, por parte del Equipo de Operación del Centro de Cómputo, los menús de depuración de registros en base de datos y reconstrucción de índices, para mantener un adecuado comportamiento en las operaciones línea y batch, previo a los cierres mensuales. Dejando como evidencia logs generados en cada proceso, que se conservan en el servidor respectivo.
Número de Control: C01
Código de Control: A13SH1801R4101C01

Proceso: P04 - Mantenimiento de Aplicaciones e Infraestructura
Código de Subproceso: SH1801
Nombre Subproceso: Actualización, Depuración y Modificación de Datos en Aplicaciones
Código Tipología de Riesgos: R4101
Riesgo: Funcionamiento inadecuado de la aplicación software
Evento de Riesgo: Indisponibilidad del servicio por altos tiempos de respuesta en procesos de consulta a las bases de datos Corporativas de aplicaciones Core (Phoenix, OpenCard, Helm Tesorería, Credismart, Datawarehouse).
Actividad de Control: Ejecutar procesos automáticos con frecuencia mensual a través de script, que regenera las estadísticas de las base de datos, para mantener un adecuado desempeño en las operaciones línea y batch. Dejando como evidencia Logs generados en cada proceso, que se conservan en el servidor respectivo.
Número de Control: C02
Código de Control: A13SH1801R4101C02

Proceso: P04 - Mantenimiento de Aplicaciones e Infraestructura
Código de Subproceso: SH1803
Nombre Subproceso: Seguimiento y Monitoreo de Aplicaciones e Infraestructura
Código Tipología de Riesgos: R1111
Riesgo: Deficiencias en inventarios
Evento de Riesgo: Riesgo de pérdida de soporte en infraestructura software base (firmware de appliances, sistemas operativos, gestores de bases de datos, servidores de aplicaciones e integradores middleware) debido a la falta de un inventario actualizado de las versiones y planes de soporte (ruta de ciclo de vida) anunciados por los proveedores de dicha infraestructura.
Actividad de Control: Validar manualmente una vez al año, por parte de los administradores de infraestructura, las versiones y planes de soporte (ruta de ciclo de vida) de infraestructura software base (firmware de appliances, sistemas operativos, gestores de bases de datos, servidores de aplicaciones e integradores middleware), mediante consulta directa a los documentos oficiales publicados o suministrados por cada proveedor (IBM, Oracle, Sybase, Microsoft, Citrix, Hewlett Packard, ACI), en los sitios web de soporte o por contacto con los mismos, dejando como evidencia documentos de resumen, con las diferentes versiones de infraestructuras en uso y las fechas de fin de soporte normal y soporte extendido, que se conservan en el servidor Sharepoint.
Número de Control: C01
Código de Control: A13SH1803R1111C01

Dirección de Monitoreo y Microinformática

Cantidad de Riesgos detectados y Controles elaborados: 3

Proceso: P04 - Mantenimiento de Aplicaciones e Infraestructura
Código de Subproceso: SH1803
Nombre Subproceso: Seguimiento y Monitoreo de Aplicaciones e Infraestructura
Código Tipología de Riesgos: R4101
Riesgo: Funcionamiento inadecuado de la aplicación software
Evento de Riesgo: Riesgo de Tecnología por malfuncionamiento de los sistemas CORE y canales transaccionales.
Actividad de Control: Monitoreo Automático y Manual de eventos configurados a nivel de infraestructura para asegurar la disponibilidad de los sistemas monitoreados (Phoenix, OpenCard) y canales transaccionales, mediante la herramienta BSM (Business Services Management) y el equipo de monitoreo que actúa con disponibilidad 7*24, dejando como evidencia reporte mensual de indicadores de disponibilidad de servicio, los cuales se conservan en el servidor SharePoint. En caso de presentarse incidencias se actuará conforme al procedimiento de seguimiento y Monitoreo sobre la Plataforma Tecnológica.
Número de Control: C01
Código de Control: A13SH1803R4101C01

Proceso: P04-Mantenimiento de aplicaciones e infraestructuras
Código de Subproceso: SH1148
Nombre Subproceso: Seguimiento al cumplimiento de los niveles de servicio
Código Tipología de Riesgos: R7101
Riesgo: Deficiencias en el servicio
Evento de Riesgo: Riesgo de proveedores por deficiencia en el servicio de mesa de ayuda de micro-informática o en los servicios de mantenimiento de equipos autoservicio (multifuncionales y depositarios).
Actividad de Control: Realizar manualmente y con frecuencia mensual por parte del Analista de Soporte Técnico, seguimiento a los niveles de servicio acordados, posterior a la generación del informe mensual, mediante reunión con los representantes del proveedor, revisando el informe presentado y tratando los siguientes aspectos: seguimiento de indicadores, revisión a las penalidades del periodo (si aplica) revisión temas y casos con sus correspondientes planes de acción, dejando como evidencia el informe mensual y acta que se conservan en servidor SharePoint. (Servicio de mesa de ayuda de micro-informática).
Número de Control: C01
Código de Control: A13SH1148R7101C01

Proceso: P04-Mantenimiento de aplicaciones e infraestructuras
Código de Subproceso: SH1148
Nombre Subproceso: Seguimiento al cumplimiento de los niveles de servicio
Código Tipología de Riesgos: R7101
Riesgo: Deficiencias en el servicio
Evento de Riesgo: Riesgo de proveedores por deficiencia en el servicio de mesa de ayuda de micro-informática o en los servicios de mantenimiento de equipos autoservicio (multifuncionales y depositarios).
Actividad de Control: Realizar Manualmente y con frecuencia mensual por parte del Analista de Soporte Técnico, seguimiento a los niveles de servicio acordados, posterior a la generación del informe mensual, mediante reunión con los representantes del proveedor, revisando el informe presentado y tratando los siguientes aspectos: seguimiento de indicadores, revisión a las penalidades del periodo (si aplica) revisión temas y casos con sus correspondientes planes de acción, dejando como evidencia el informe mensual y acta que se conservan en servidor SharePoint . (Servicios de mantenimiento de equipos autoservicio).
Número de Control: C02
Código de Control: A13SH1148R7101C02

Dirección del Centro de Procesamiento de Datos

Cantidad de Riesgos detectados y Controles elaborados: 7

Proceso: P04 - Mantenimiento de Aplicaciones e Infraestructura
Código de Subproceso: SH1146
Nombre Subproceso: Seguimiento a la administración de los datos (Respaldo, Restauración, Eliminación y custodia)
Código Tipología de Riesgos: R4104
Riesgo: Almacenamiento imposibilidad de recuperación de datos
Evento de Riesgo: Riesgo de Imposibilidad de restaurar Datos por cintas dañadas ó defectuosas, o debido a la no parametrización en la herramienta de backups de las políticas de respaldo.
Actividad de Control: Ejecutar para fechas aleatorias, labores de restauración de cintas, con el fin de validar la integridad de las mismas. Ésta actividad se realiza trimestralmente por parte del Administrador de Medios del equipo de Procedatos, dejando como evidencia logs que se conservan en medio magnético en el servidor de Sharepoint y en caso de inconsistencias, solicitar al responsable de medios su atención inmediata.
Número de Control: C01
Código de Control: A13SH1146R4104C01

Proceso: P04 - Mantenimiento de Aplicaciones e Infraestructura
Código de Subproceso: SH1146
Nombre Subproceso: Seguimiento a la administración de los datos (Respaldo, Restauración, Eliminación y custodia)
Código Tipología de Riesgos: R4104
Riesgo: Almacenamiento imposibilidad de recuperación de datos
Evento de Riesgo: Riesgo de Imposibilidad de restaurar Datos por cintas dañadas ó defectuosas, o debido a la no parametrización en la herramienta de backups de las políticas de respaldo.
Actividad de Control: Garantizar por parte del Jefe Procedatos la correcta parametrización de las políticas de respaldos y que todo el sistema productivo sea respaldado periódicamente, actividad realizada trimestralmente previo a la operación, mediante revisión de las políticas de respaldo, dejando como evidencia informe mensual que se conserva en medio magnético en el Servidor de Sharepoint.
Número de Control: C02
Código de Control: A13SH1146R4104C02

Proceso: P04 - Mantenimiento de Aplicaciones e Infraestructura
Código de Subproceso: SH1146
Nombre Subproceso: Administración del Procesamiento de Datos
Código Tipología de Riesgos: R4101
Riesgo: Funcionamiento inadecuado de la aplicación software
Evento de Riesgo: Riesgo de Cierre ejecutado de manera incorrecta, debido a la no ejecución del proceso, de acuerdo al orden establecido.
Actividad de Control: Asegurar manualmente y a diario por parte del Coordinador de Procedatos, la disponibilidad de la planilla de ejecución de procesos debidamente actualizada, previo al inicio de las labores de cierre diario, dejando como evidencia bitácoras de Proceso y Patrón de procesos, que se conservan en medio magnético en el servidor de Sharepoint, así mismo se conservan en medio físico las planillas.
Número de Control: C01
Código de Control: A13SH1146R4101C01

Proceso: P06 - Gestión de la Seguridad Física y Lógica
Código de Subproceso: SH1123
Nombre Subproceso: Administración de la Seguridad Física en Centros de Cómputo
Código Tipología de Riesgos: R3201
Riesgo: Uso indebido de poderes o limites
Evento de Riesgo: Riesgo de pérdida de la integridad de la información en Producción debido a acceso al Data Center por parte de personal no autorizado.

Actividad de Control: Validar y analizar manualmente, con frecuencia trimestral por parte del Jefe Procedatos, los accesos a las instalaciones del data center de calle 27 y mantener un registro único y preciso de todas las Solicitudes Aprobadas y Rechazadas de acceso previo a la operación, mediante verificación de las planillas y archivos de acceso, dejando como evidencia planilla física de los accesos al sitio y archivo con información del sistema de seguridad centralizado y administrado por Seguridad Física. Éstos se conservan en medio magnético y en caso de inconsistencias revisar con el área de seguridad el incidente para generar la medida respectiva de control.
Número de Control: C01
Código de Control: A13SH1123R3201C01

Proceso: P06 - Gestión de la Seguridad Física y Lógica
Código de Subproceso: SH1802
Nombre Subproceso: Gestión de la Seguridad Física y Lógica
Código Tipología de Riesgos: R4103
Riesgo: Fallo del sistema e interrupción del Negocio Hardware
Evento de Riesgo: Riesgo de Pérdida de información en Producción debido a factores ambientales o de eventos que afecten el normal desarrollo de las operaciones, daños en equipos y continuidad de los sistemas del Banco.
Actividad de Control: Revisar manualmente y a diario por parte del Jefe Procedatos, el medio ambiente dentro del CPD de calle 27 y establecer medidas de control ambiental para el Centro de Procesamiento de Datos (CPD), previo a la operación, mediante verificación con recorrido físico. Dejando como evidencia informe mensual de las condiciones ambientales del CPD (disponibilidad de aires, energía) que se conserva en Servidor Sharepoint y en caso de inconsistencias generar incidente al área encargada para su solución.
Número de Control: C01
Código de Control: A13SH1802R4103C01

Proceso: P06 - Gestión de la Seguridad Física y Lógica
Código de Subproceso: SH1802
Nombre Subproceso: Gestión de la Seguridad Física y Lógica
Código Tipología de Riesgos: R4103
Riesgo: Fallo del sistema e interrupción del Negocio Hardware
Evento de Riesgo: Riesgo de Pérdida de información en Producción debido a factores ambientales o de eventos que afecten el normal desarrollo de las operaciones, daños en equipos y continuidad de los sistemas del Banco.
Actividad de Control: Gestionar y garantizar por parte del Jefe de Procedatos, el cumplimiento del plan de mantenimiento definido para la infraestructura eléctrica que soporta la operación del Datacenter de la Calle 27. El plan de mantenimiento se ejecuta 3 veces al año por parte del Proveedor contratado para tal fin, mediante mantenimiento preventivo y correctivo de plantas y ups, dejando como

evidencia los registros que se conservan en servidor Sharepoint y en caso de inconsistencias solicitar al área de inmuebles su solución inmediata.
Número de Control: C02
Código de Control: A13SH1802R4103C02

Proceso: P07 - Gestión del Plan de Continuidad del Negocio
Código de Subproceso: SH1125
Nombre Subproceso: Gestión del Plan de Continuidad del Negocio
Código Tipología de Riesgos: R6103
Riesgo: Ausencia o deficiencia de planes de contingencia
Evento de Riesgo: Riesgo de no restablecer el servicio en Producción debido a que frente a una contingencia no se cuenta con un procedimiento claro de cómo actuar para restablecer el servicio.
Actividad de Control: Asegurar el cumplimiento de las pruebas de DRP para los sistemas críticos establecidos por el BIA, actividad coordinada por el Jefe Procedatos, mediante seguimiento de actividades y coordinación de pruebas semestrales, dejando como evidencia los informes de pruebas que se conservan en medio magnético en el Servidor de Sharepoint.
Número de Control: C01
Código de Control: A13SH1125R6103C01

Dirección de Telecomunicaciones

Cantidad de Riesgos detectados y Controles elaborados: 1

Proceso: P04-Mantenimiento de aplicaciones e infraestructuras
Código de Subproceso: SH1148
Nombre Subproceso: Seguimiento al cumplimiento de los niveles de servicio
Código Tipología de Riesgos: R7101
Riesgo: Deficiencias en el servicio prestado
Evento de Riesgo: Riesgo de proveedores por deficiencia en los servicios de telecomunicaciones.
Actividad de Control: Realizar manualmente y con frecuencia mensual por parte del Jefe de comunicaciones, seguimiento a los niveles de servicio acordados posterior a la generación del informe mensual, mediante reunión con los representantes del proveedor, revisando el informe presentado y tratando los siguientes aspectos: seguimiento de indicadores, revisión de incidentes relevantes y sus correspondientes planes de acción, revisión a las penalidades del periodo (si aplica), dejando como evidencia el informe mensual y acta recibida por correo electrónico que se conservan en servidor SharePoint
Número de Control: C03
Código de Control: A13SH1148R7101C03

5.3.4 Proceso de Auditoría Interna y seguimiento. Con éste proceso de Auditoría Interna se pretende realizar una revisión inicial detallada de las actividades de control y sus respectivas evidencias en cada una de las Direcciones de la Gerencia de Producción, antes de realizar la selección aleatoria de las Pruebas de Controles Sox.
Esta Auditoría ayuda en gran medida para que cada Dirección ó cada Área de Tecnología evalúe internamente si los Controles propuestos están siendo cumplidos por los funcionarios satisfactoriamente y mantienen todos los soportes y evidencias correspondientes, ó por el contrario, se está haciendo caso omiso a los Controles propuestos ó se establecieron controles difíciles de cumplir, por lo cual se tendrían que reevaluar en el siguiente semestre de certificación.

Respecto a las Pruebas de Controles Sox existen 3 tipos de evaluación aplicables a realizar para cada control:

Auto-evaluación: En este caso, las pruebas de efectividad las realizan los propios responsables del control ó personal de la misma área.

Pruebas cruzadas: En este caso, las pruebas cruzadas son realizadas por personal diferente al responsable del control y sin ningún tipo de relación jerárquica con éste (Personas de otra área).

No aplica: Utilizado sólo si durante el período a certificar, no se presentó operativa relacionada con el control establecido

La Auditoría interna se dividió en 2 fases:

Fase I: En éste ejercicio de Auditoría Interna, se realizaron pruebas cruzadas únicamente con 2 de las 5 Direcciones de la Gerencia de Producción (Dirección de Monitoreo y Microinformática y Dirección de Telecomunicaciones) por la premura de tiempo. Ésta consiste en que se realiza auditoría a una Dirección diferente a la propia y se verifican las actividades de control y las evidencias existentes de otra Dirección, con el fin de encontrar inconsistencias si las hay y corregirlas a tiempo ó complementar las evidencias si es el caso.

Fase II: En éste ejercicio de Auditoría Interna, se realizaron pruebas de Auto-evaluación, en las que cada Dirección se tomó el tiempo de verificar que sus propios controles estuvieran siendo aplicados y contaran con los soportes y evidencias necesarios para el periodo comprendido de certificación.

El Autor, quien hace parte de la Dirección de Aseguramiento de Calidad, estuvo encargado de liderar las pruebas de autoevaluación, pero como la muestra era tan extensa por la periodicidad del control que es en cada operación, se propuso realizar un plan de choque con la totalidad de funcionarios del Área en un horario no hábil, para revisar en detalle que las actividades de control cumplieran con lo

establecido en los procedimientos respectivos y existieran las evidencias correspondientes.

5.3.4.1 Resultado de la Auditoría Interna. El resultado de ésta auditoría interna para la Dirección de Aseguramiento de Calidad fue el siguiente:
a) Control de Cambios rutinarios: Se tomaron muestras con periodicidad “en cada operación”. Para este control la totalidad de la muestra es de 1.511 controles de cambios para el año 2014. De acuerdo a la metodología se establece realizar una muestra de 45 controles de cambio para el año 2014.

b) Control de cambios menores o modificación de datos: Se tomaron muestras con periodicidad “en cada operación”. Para este control la totalidad de la muestra es de 1.511 controles de cambio para el año 2014. De acuerdo a la metodología se establece realizar una muestra de 45 controles de cambio para el año 2014, el mismo número de cambios pero con una muestra diferente.

c) Solicitudes de prueba - Visto Bueno: Se tomaron muestras con periodicidad “en cada operación”. Para este control la totalidad de la muestra es de 621 controles de cambio para el año 2014. De acuerdo a la metodología se establece realizar una muestra de 45 controles de cambio para el año 2014.

d) Solicitudes de prueba - Con pruebas de área: Se tomaron muestras con periodicidad “en cada operación”. Para este control la totalidad de la muestra es de 621 controles de cambio para el año 2014. De acuerdo a la metodología se establece realizar una muestra de 45 controles de cambio para el año 2014, el mismo número de cambios pero con una muestra diferente.

e) Catalogación y versionamiento de solicitudes de prueba: Se tomaron muestras con periodicidad “en cada operación”. Para este control la totalidad de la muestra es de 621 controles de cambio para el año 2014. De acuerdo a la metodología se establece realizar una muestra de 45 controles de cambio para el año 2014.

Finalizado éste ejercicio de auditorías internas, se recomendó realizar un seguimiento trimestral al cumplimiento del total de los Controles Propuestos en la Gerencia de Producción, de manera que se vayan evaluando las actividades de control en cada actividad y operación realizada y no sólo en las visitas de Certificación Sox.

5.3.5 Proceso de Pruebas de efectividad de los Controles. Se realizó un proceso interesante en la ejecución pruebas de Controles Sox. Para ésta actividad se corren algunas macros en Excel que realizan una selección aleatoria de acuerdo a un cuadro de muestreo y una población. Dentro de estas pruebas se debe señalar la periodicidad del control, el tamaño de la población, la frecuencia y el tamaño de la muestra anual. Con la selección aleatoria resultado se realiza un

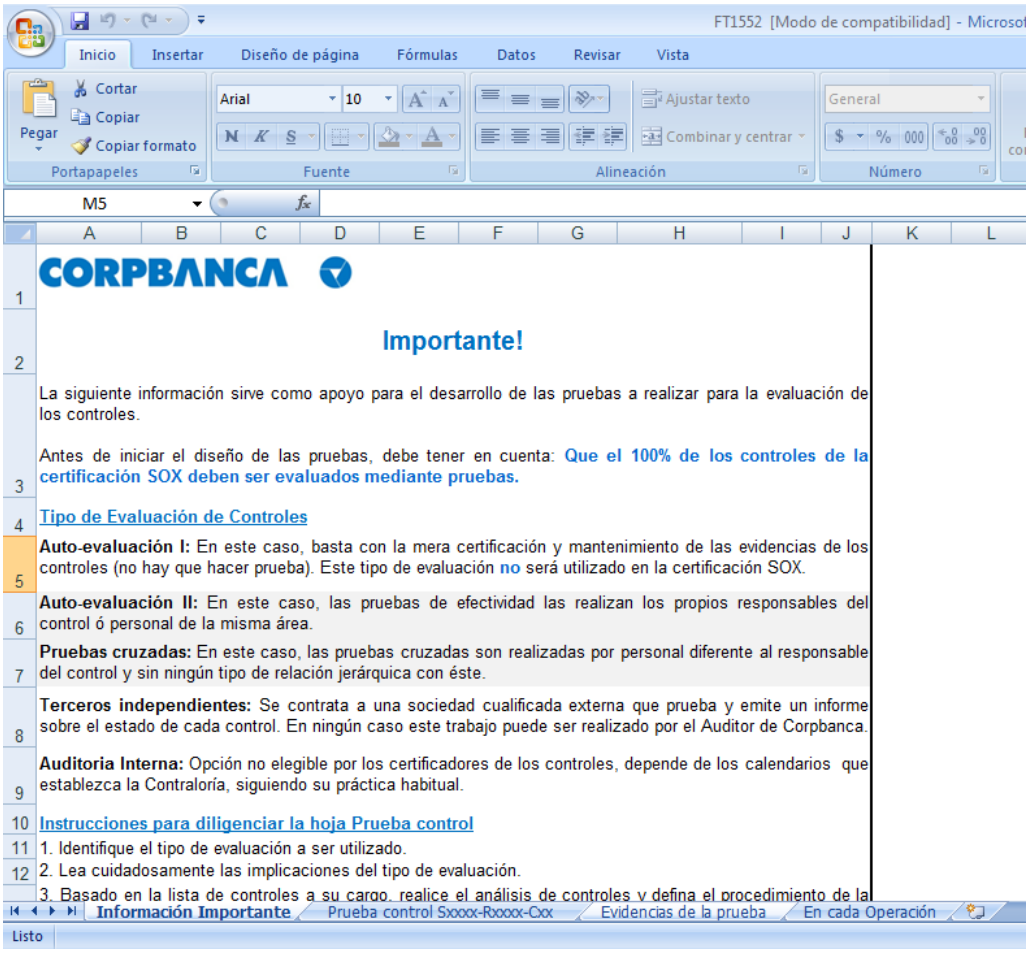
filtro y se debe verificar uno a uno que la evidencia de la muestra se encuentre en el servidor destinado para ello.

Finalmente se realiza un análisis en el cual se verifica que si para toda la muestra la evidencia de la actividad de control existe, esa actividad de control es exitosa, pues por una sola evidencia que falte, el Control se considera No Efectivo. En caso de que un Control resulte No Efectivo, se debe redactar el plan de acción dentro del Formato FT1552 Prueba Controles MCI-SOX.

La utilización del formato FT1552 Prueba Controles MCI-SOX que se muestran en las Figuras 9, 10, 11 y 12, es de uso obligatorio para todos los controles a certificar ya que en el queda registrada la información de pruebas de cada control, los resultados de la muestra y si es ó no efectivo. Éste formato está compuesto por 4 hojas con campos requeridos y lo diligencia la persona que estuvo a cargo de efectuar la prueba para la evaluación de los controles.

Hoja1 – Información Importante
Contiene el Tipo de Evaluación de Controles
Contiene las instrucciones para diligenciar la hoja prueba control

Figura 9. Formato de Pruebas de Control Sox - FT1552 - Hoja Información Importante

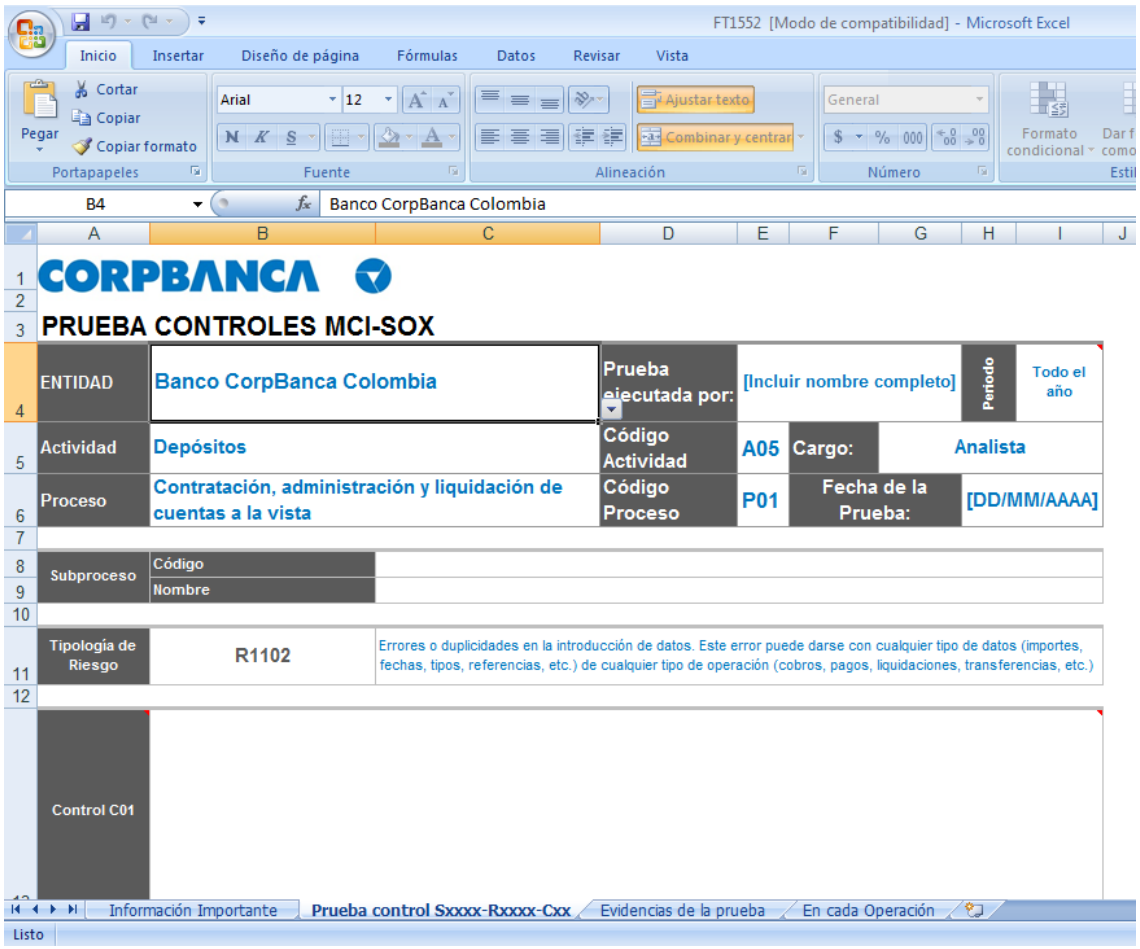


Fuente Banco Corpbanca Colombia.

Hoja2 – Resultado Pruebas Control

En ésta hoja se diligencia toda la información correspondiente a las pruebas del Control, además del nombre del responsable de la ejecución de la prueba y fecha, Código de Proceso, Subproceso, Tipología de Riesgo, el Control, Tipo de Prueba ejecutada, Periodicidad del Control, tamaño de la muestra anual, nombre de la evidencia, conclusión de la prueba, plan de acción y Responsable y fecha del plan de acción. Contiene también la macro en la cual se realiza la selección de muestras aleatoriamente.

Figura 10. Formato de Pruebas de Control Sox – FT1552 - Hoja Prueba Control

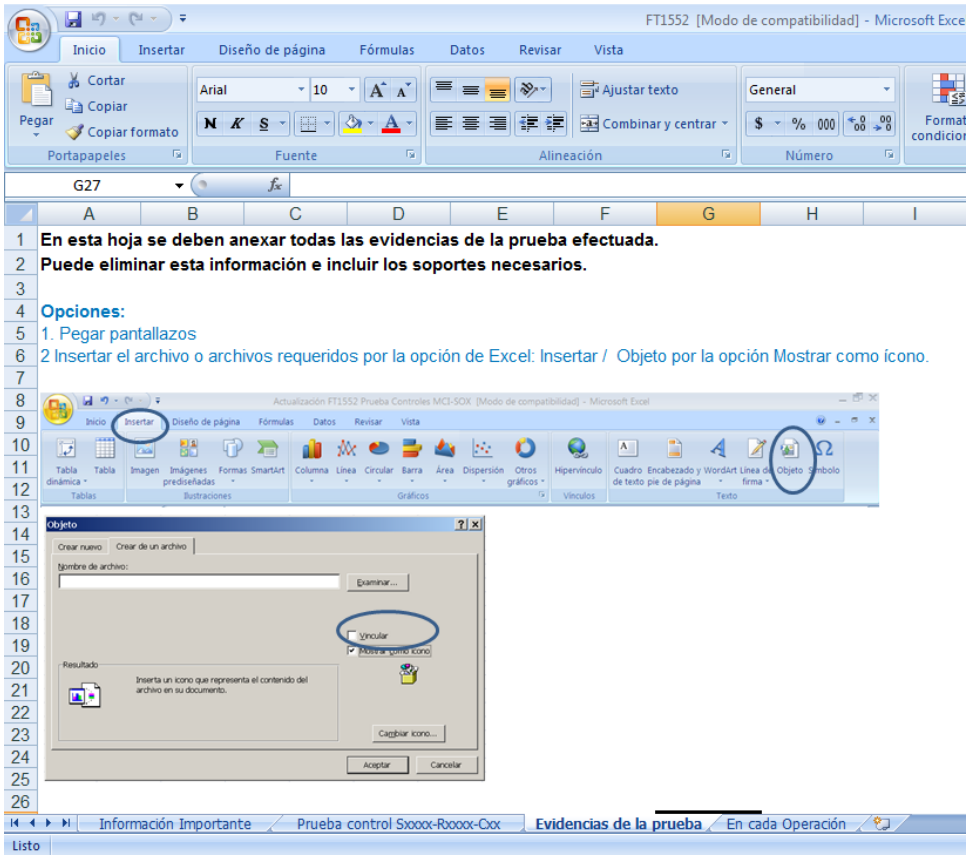


Fuente Banco Corpbanca Colombia.

Hoja3 – Evidencia de la Prueba

Allí se deja la ruta donde fue dejada la evidencia ó las pantallas de la evidencia según el tamaño de la muestra analizada.

Figura 11. Formato de Pruebas de Control Sox – FT1552 – Hoja Evidencia de las Pruebas

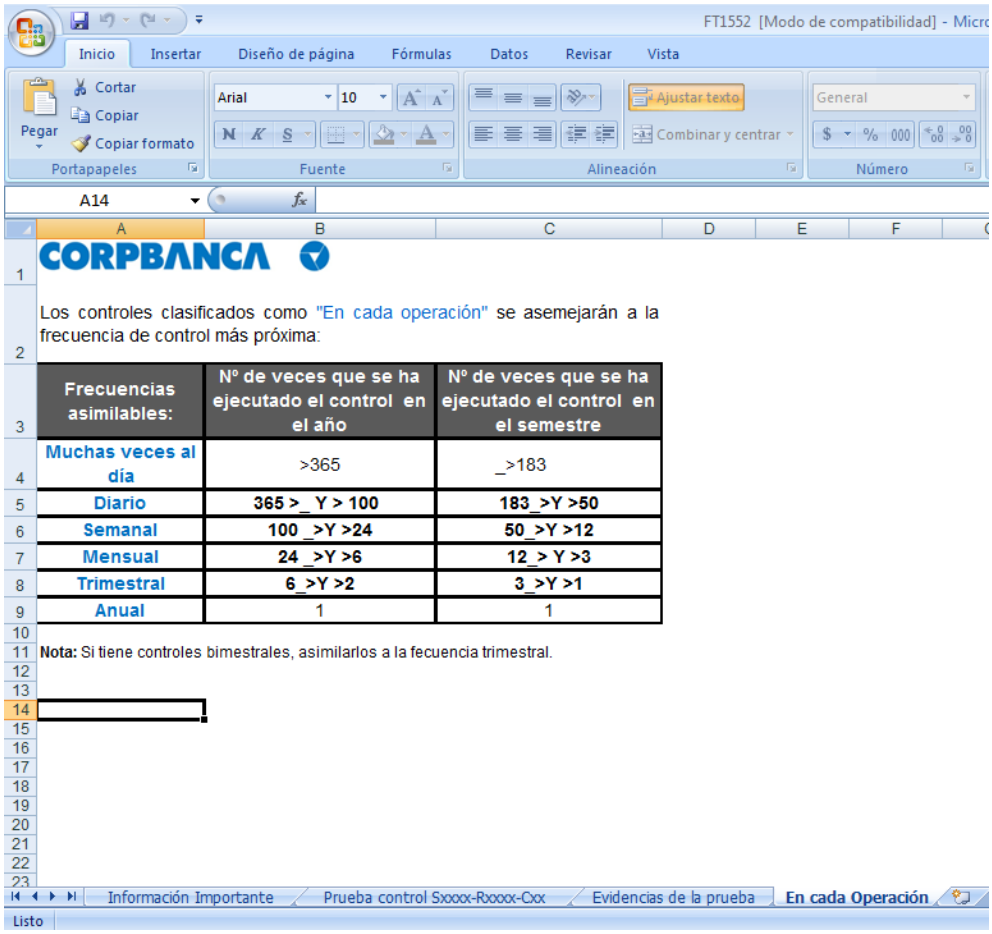


Fuente Banco Corpbanca Colombia.

Hoja4 - En cada operación

En ésta hoja se encuentra una tabla informativa con la frecuencia asimilable, unos rangos con el número de veces que se ha ejecutado el control en el año y en el semestre para obtener el tamaño de la muestra para los controles cuya frecuencia es “En cada operación”. De acuerdo a ésta tabla se colocan los valores en la macro para seleccionar la muestra.

Figura 12. Formato de Pruebas de Control Sox – FT1552 – Hoja En cada operación



Fuente Banco Corpbanca Colombia.

En cada hoja se encuentran bloqueadas las celdas en las que el elaborador de la prueba no debe efectuar modificaciones, dejando así disponibles sólo las celdas en las que se requiere incluir algún tipo de información.

Así que es necesario tener en cuenta la operatividad de los controles para la selección de las muestras requeridas para la prueba. Por ejemplo, si el control fue vigente hasta Mayo 2014, la muestra debe cubrir los primeros cinco meses del 2014, si a raíz de este cambio y por temas de fusión surgió un nuevo control, la muestra debe cubrir de Junio a Diciembre de 2014. Al efectuar las pruebas debe garantizarse el cubrimiento de todo el año 2014.

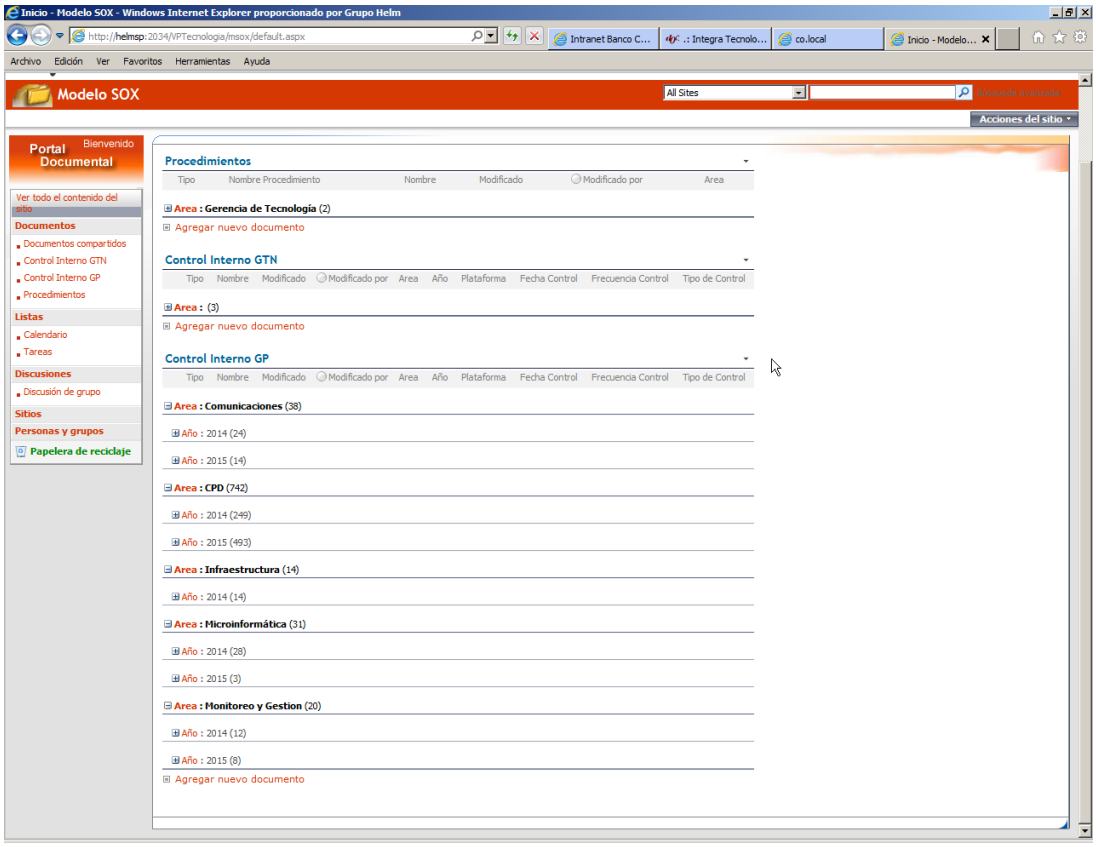
Luego de verificar los resultados de las pruebas de Controles SOX en las 5 Direcciones de la Gerencia de Producción, se encontraron 2 Controles No Efectivos para la Dirección de Infraestructura por evidencia insuficiente.

5.4 EVIDENCIAS

Las evidencias juegan un papel bien importante en el Sistema de Control Interno, ya que son la mejor forma de garantizar por parte del Auditor, que las Actividades de Control propuestas en un Área se están atendiendo y como resultado de una buena labor se conservan las evidencias soportes.

Como se observa en la Figura 13. Ruta de Evidencias Año 2014 de las 5 Direcciones de la Gerencia de Producción, la mayoría de las evidencias fueron colocadas en una ruta del servidor documental con la Herramienta Sharepoint.

Figura 13. Ruta de Evidencias Año 2014 de las 5 Direcciones de la Gerencia de Producción



Fuente Banco Corpbanca Colombia.

Varias de ésas evidencias están compuestas por:

- ✓ Reportes
- ✓ Informes
- ✓ Manuales
- ✓ Planillas de Cierres
- ✓ Logs de Auditoría
- ✓ Soportes Cambios a producción
- ✓ Aprobaciones de Directivos
- ✓ Actas celebradas con Proveedores

5.5 EVALUACIÓN Y EFECTIVIDAD DE LOS CONTROLES

De las 20 Actividades de Control de la Gerencia de Producción, finalmente quedaron 2 Controles como No Efectivos con las siguientes observaciones y plan de implementación:

"Control A13SH1801R4101C01 no efectivo, por evidencia insuficiente. Se aclara que este control se ha ejecutado en la periodicidad definida, sin embargo los Logs se sobreescribían cada mes, ocasionando la pérdida de evidencias.
Plan de implementación para asegurar registro permanente de evidencias: Fase I: Noviembre 30 de 2014 y Fase II: Marzo 30 de 2015."

"Control A13SH1801R4101C02 no efectivo, por evidencia insuficiente. Se aclara que este control se ha ejecutado en la periodicidad definida, sin embargo los Logs se sobreescribían cada mes, ocasionando la pérdida de evidencias.
Plan de implementación para asegurar registro permanente de evidencias: Implementado desde Noviembre 30 de 2014."

En el Mes de Marzo 2015 se logró finalizar la Certificación de todo el Año 2014 y actualmente se está realizando seguimiento y evaluación de los controles propuestos para el 1er. Semestre 2015.

De ésta manera, se realiza con completo éxito la Implementación de un Sistema de Control Interno en Helm Bank, al igual que la identificación, evaluación y análisis de Riesgos y elaboración de Actividades de Controles Internos en las 5 Direcciones que conforman la Gerencia de Producción a nivel de Tecnología.

5.6 PROCESO DE CERTIFICACIÓN

El proceso de certificación se realiza cuando se entrega a la Gerencia de Riesgo Operativo y Seguridad la cantidad de Formatos FT1552 - Prueba de Controles

SOX diligenciados en su totalidad, por cada uno de los Controles elaborados (Para la Gerencia de Producción se realizó la entrega de 20 Formatos FT1552 diligenciados).

Se entrega la Matriz SOX consolidada en formato Excel y en la primera hoja con nombre “Certificación Banco” se detalla la información del País, el nombre de la Entidad Financiera, códigos de los controles, nombre, cargo, número de cédula y firma del Gerente del área, comentarios de los controles No Efectivos con su plan de acción y fecha de la firma. La hoja de Certificación también debe ser impresa y escaneada y firmada en original por el Gerente del área.

Estos documentos se entregan vía correo electrónico a la cuenta de correo de la Gerencia de Riesgo Operativo y Seguridad. Posteriormente, la Gerencia de Riesgo Operativo y Seguridad se encarga de entregar ésta misma información al Presidente Ejecutivo y Financiero para su correspondiente revisión de resultados y firma. Para ello existe una carta de certificación en la cual se resumen todos los resultados de las diferentes áreas del Banco como de las Filiales.

Finalmente, toda ésta información de las áreas del Banco que se certificaron en Controles Sox, es consolidada y enviada a Banco Corpbanca en Casa Matriz Chile, en un informe con nombre 20F, que contiene alrededor de 900 páginas y desde allí es enviada a la SEC en los Estados Unidos.

5.7 CAPACITACIONES

Periódicamente se desarrolla un proceso de capacitación presencial y/o virtual sobre control interno y riesgo operativo, basado en ejemplos de casos reales con el fin de sensibilizar a todos los integrantes del Grupo Corpbanca Colombia, enfatizando en que en toda labor realizada existen riesgos operativos que debemos mitigar para evitar pérdidas para nuestra entidad. Estas campañas buscan que los empleados contribuyan con la identificación de los riesgos aportando controles para la minimización de los mismos.

6. CRONOGRAMA

6.1 ACTIVIDADES DEL CRONOGRAMA

Durante la implementación del Sistema de Control Interno (SCI) en la Gerencia de Producción, fue necesario ajustar algunas fechas del Cronograma propuesto inicialmente en el Anteproyecto por factores como la fecha límite de certificación final que era desconocida, la fecha de entrega de la Certificación por parte del Gerente de Producción a la Vicepresidencia de Riesgo y Casa Matriz y también por las fechas de entrega del Trabajo de Grado a la Universidad Piloto de Colombia, como se encuentra en la Figura 14.

Se adjunta cronograma actualizado con las actividades realizadas en el periodo 2014- 2015.

Figura 14. Cronograma en Project Desarrollo de Proyecto Implementación SCI en Helm Bank

	Nombre de tarea	Duración	% completado	Comienzo	Fin
1	**Cronograma Implementación Sistema de Control Interno SOX - Gerencia de Producción**	**271 días**	**99%**	**vie 10/10/14**	**jue 19/11/15**
2	**Preparación proceso de Implementación**	**24 días**	**100%**	**vie 10/10/14**	**vie 14/11/14**
3	Planeación de la implementación de SCI en la Gerencia de Producción.	5 días	100%	vie 10/10/14	vie 17/10/14
4	Levantamiento de información de riesgos actuales en las 5 Direcciones de la Gerencia de Producción	6 días	100%	mié 22/10/14	mié 29/10/14
5	Consolidación de la información	1 día	100%	jue 30/10/14	jue 30/10/14
6	Revisión de procesos, subprocesos y procedimientos actuales	3 días	100%	vie 31/10/14	mié 05/11/14
7	Revisión de códigos de Procesos, Subprocesos, Procedimientos y Tipologías de Riesgos	3 días	100%	jue 06/11/14	lun 10/11/14
8	Revisión de la Cadena de Valor a nivel de la Vicepresidencia de Tecnología	2 días	100%	mar 11/11/14	mié 12/11/14
9	Revisar actividades realizadas en Direcciones GP y verificar existencia de Políticas, Normas y Procedimientos	2 días	100%	jue 13/11/14	vie 14/11/14
10	**Identificación, evaluación y elaboración de riesgos en las 5 Direcciones de la Gerencia de Producción.**	**205 días**	**100%**	**mar 20/01/15**	**jue 19/11/15**
11	Riesgos Dirección de Aseguramiento de Calidad	2 días	100%	mié 18/11/15	jue 19/11/15
12	Riesgos Dirección de Infraestructura	2 días	100%	mar 20/01/15	mié 21/01/15
13	Riesgos Dirección de Monitoreo y Microinformática	2 días	100%	jue 22/01/15	vie 23/01/15
14	Riesgos Dirección del Centro de Procesamiento de Datos	2 días	100%	lun 26/01/15	mar 27/01/15
15	Riesgos Dirección de Telecomunicaciones	2 días	100%	mié 28/01/15	jue 29/01/15
16	**Construcción de Controles Internos en las 5 Direcciones de la Gerencia de Producción.**	**11 días**	**82%**	**vie 30/01/15**	**vie 13/02/15**
17	Controles Dirección de Aseguramiento de Calidad	2 días	100%	vie 30/01/15	lun 02/02/15
18	Controles Dirección de Infraestructura y Dirección de Telecomunicaciones	4 días	50%	mar 03/02/15	vie 06/02/15
19	Controles Dirección de Monitoreo y Microinformática	2 días	100%	lun 09/02/15	mar 10/02/15
20	Controles Dirección del Centro de Procesamiento de Datos	2 días	100%	mié 11/02/15	jue 12/02/15
21	Atender visita de Auditoría Interna - Evaluación de los controles SOX	1 día	100%	vie 13/02/15	vie 13/02/15
22	**Proceso de Certificación SOX**	**72 días**	**100%**	**vie 13/02/15**	**vie 29/05/15**
23	Realizar auditorías cruzadas	3 días	100%	vie 13/02/15	mar 17/02/15
24	Verificar la existencia de las evidencias en el Servidor de las Direcciones de la Gerencia de Producción	2 días	100%	mar 17/02/15	mié 18/02/15
25	Tomar muestras para las pruebas de Controles SOX	2 días	100%	jue 19/02/15	vie 20/02/15
26	Realizar Auditoría Auto-evaluación para la Dirección de Aseguramiento de Calidad	4 días	100%	sáb 21/02/15	mié 25/02/15
27	Verificar los resultados de las pruebas de Controles SOX	4 días	100%	mar 24/02/15	vie 27/02/15
28	Diligenciar el Formato FT1552 - Prueba de controles SOX	2 días	100%	lun 02/03/15	mar 03/03/15
29	Reuniones de Seguimiento Pre-Certificación	1 día	100%	mié 04/03/15	mié 04/03/15
30	Diligenciamiento de la Matriz SOX general	2 días	100%	mié 04/03/15	jue 05/03/15
31	Aprobación de Matriz SOX final por cada Dirección	1 día	100%	vie 06/03/15	vie 06/03/15
32	Entrega de Matriz SOX a las Áreas de Riesgo Operativo y Seguridad	1 día	100%	lun 09/03/15	lun 09/03/15
33	Certificación por parte de la Gerencia de Producción	1 día	100%	lun 09/03/15	lun 09/03/15
34	Entrega de Certificación y Formatos FT1552 - Prueba de controles SOX diligenciados	1 día	100%	lun 09/03/15	lun 09/03/15
35	Seguimiento al cumplimiento de los Controles Propuestos en la Gerencia de Producción	5 días	100%	lun 25/05/15	vie 29/05/15
36	**Trabajo de Grado**	**112 días**	**100%**	**lun 01/06/15**	**vie 13/11/15**
37	Elaboración documento Trabajo de Grado - Revisión Tutor de la Universidad Piloto de Colombia	30 días	100%	lun 01/06/15	mié 15/07/15
38	Elaboración documento Trabajo de Grado Final - Revisión Tutor de la Universidad Piloto de Colombia	69 días	100%	lun 03/08/15	mié 11/11/15
39	Elaboración del Artículo para entregar en la Universidad Piloto de Colombia	30 días	100%	mar 29/09/15	mié 11/11/15
40	Entrega Final Trabajo de Grado Universidad Piloto de Colombia	1 día	100%	vie 13/11/15	vie 13/11/15

Fuente Elaborado por el Autor

7. CONCLUSIONES

- ✓ Un proceso de certificación tan importante como lo es el de la Ley Sox, es de vital importancia para toda Organización porque genera un alto nivel de compromiso y responsabilidad de las áreas en mejorar sus funciones diarias.

- ✓ Las incidencias que se generan en la ejecución de un proceso de prueba Sox ayudan al mejoramiento continuo para detectar posibles eventos de riesgo que no han sido cubiertos y a redefinir y fortalecer los controles.

- ✓ Fue satisfactorio realizar una gestión adecuada para detectar, analizar y evaluar los riesgos relevantes presentados en la Gerencia de Producción y definir actividades de control de acuerdo a los Procesos, Subprocesos y Procedimientos existentes.

- ✓ La prevención y disminución de ocurrencia de fraudes originados tanto al interior como al exterior de la Entidad, solo pueden ser posibles con un adecuado tratamiento de los riesgos críticos detectados en las diferentes áreas de la Organización.

8. RECOMENDACIONES

- ✓ Toda actividad que sea realizada por parte de los funcionarios de la Gerencia de Producción debe ser efectuada con disciplina para que no se presenten fallas en las auditorías internas que luego darán paso a la siguiente certificación Sox.

- ✓ Realizar un seguimiento trimestral al cumplimiento del total de los Controles Propuestos en la Gerencia de Producción, de manera que se vayan evaluando las actividades de control en cada actividad y operación realizada y no sólo en las visitas de Certificación Sox.

- ✓ Es recomendable que en las 5 Direcciones de la Gerencia de Producción se realice actualización en las normas, políticas y procedimientos de los Procesos de Tecnología, de acuerdo a las funciones realizadas por los funcionarios encargados y mencionar de manera puntual cual es la reacción en caso de presentarse una incidencia.

- ✓ Continuar realizando campañas de sensibilización a todos los funcionarios del Grupo Financiero y especialmente a las diferentes áreas de la Vicepresidencia de Tecnología, pues de las buenas prácticas de sus funciones, depende que los resultados de las Auditorías Internas y Externas para la Certificación Sox, sean exitosas en cada semestre del año.

9. REFERENCIAS BIBLIOGRÁFICAS

BANCO CORPBANCA COLOMBIA S.A., Intranet Corporativa, Herramienta DocManager, Sección Manuales, Bogotá, Octubre 2015

BANCO CORPBANCA COLOMBIA S.A., Escuela Virtual Corpbanca, Cursos Normativos 2015, Módulo PCN 2015 y Seguridad de la Información (PCN2015), Bogotá, Agosto 2015

BANCO CORPBANCA COLOMBIA S.A., Escuela Virtual Corpbanca, Cursos Normativos 2015, Módulo SARO, Bogotá, Agosto 2015

BANCO CORPBANCA COLOMBIA S.A., SP1309 Subproceso Incidencias y Planes de Acción del Modelo de Control Interno SOX, Última fecha publicación 15 de Septiembre de 2015, Versión 7, Código SP1309, Publicado en Herramienta de Gestión Documental - Aplicativo “DocManager”

BANCO CORPBANCA COLOMBIA S.A., SP1310 Subproceso Valoración del Riesgo Operativo, Última fecha publicación 22 de Diciembre de 2015, Versión 5, Código SP1310, Publicado en Herramienta de Gestión Documental - Aplicativo “DocManager”

BANCO CORPBANCA COLOMBIA S.A., SP1313 Subproceso Gestión Proceso de Certificación Modelo de Control Interno SOX, Última fecha publicación 15 de Septiembre de 2015, Versión 9, Código SP1313, Publicado en Herramienta de Gestión Documental - Aplicativo “DocManager”

BANCO CORPBANCA COLOMBIA S.A.,MG1012 Manual General Gestión de Procesos Modelo de Control Interno, Última fecha publicación 27 de Junio de 2015, Versión 4, Código MG1012, Publicado en Herramienta de Gestión Documental - Aplicativo “DocManager”

BANCO CORPBANCA COLOMBIA S.A., Gerencia de Riesgo Operacional y Seguridad, Sistema de Control Interno Modelo SOX Corpbanca-Helm, [diapositivas Presentación Final Gerentes.pptx], Bogotá, Febrero de 2014

BANCO CORPBANCA COLOMBIA S.A., Gerencia de Riesgo Operacional y Seguridad, Actualización COSO 2013 Vicepresidencia de Tecnología, [diapositivas COSO actualización tecnología.pptx], Bogotá, Agosto de 2015

BANCO CORPBANCA COLOMBIA S.A., Gerencia de Riesgo Operacional y Seguridad, Guía de Certificación de Controles MCI-SOX Vicepresidencia de Riesgo, [diapositivas Guía de Certificación de Controles MCI-SOX Dic 2014.pdf], Bogotá, 18 de Febrero de 2015

BANCO CORPBANCA COLOMBIA S.A., Gerencia de Riesgo Operacional y Seguridad, [Formato FT1494 Matriz de Riesgos y Controles SOX.xls], Bogotá, 01 de Octubre de 2015

BANCO CORPBANCA COLOMBIA S.A., Gerencia de Riesgo Operacional y Seguridad, [Formato FT1552 Prueba Controles MCI-SOX.xls], Bogotá, 01 de Octubre de 2015

HERNÁNDEZ MOLINA. Ignacio. La Formulación de Proyectos en Ciencias e Ingenierías, primera edición, Bogotá, Colombia, 2012, págs. 83-105, 117-126, 129-143, 171-187, 217-236

NORMA TÉCNICA COLOMBIANA. Presentación de tesis, trabajos de grado y otros trabajos de investigación. Bogotá: ICONTEC, 2008. Sexta actualización (NTC 1486)

U.S. SECURITIES AND EXCHANGE COMMISSION. [En línea]. Última modificación 14 de Abril de 2015. Disponible en Internet:<http://secsearch.sec.gov/search?utf8=%E2%9C%93&affiliate=secsearch&query=section+404+sarbanes+oxley> [citado en 14 de Diciembre 2015]